

The New York Times Reprints

This copy is for your personal, noncommercial use only. You can order presentation-ready copies for distribution to your colleagues, clients or customers here or use the "Reprints" tool that appears next to any article. Visit www.nytreprints.com for samples and additional information. Order a reprint of this article now.

March 22, 2012

Read 10/18 in class

U.S. Relaxes Limits on Use of Data in Terror Analysis

By CHARLIE SAVAGE

WASHINGTON — The Obama administration is moving to relax restrictions on how counterterrorism analysts may retrieve, store and search information about Americans gathered by government agencies for purposes other than national security threats.

Attorney General Eric H. Holder Jr. on Thursday signed new guidelines for the National Counterterrorism Center, which was created in 2004 to foster intelligence sharing and serve as a terrorism threat clearinghouse.

The guidelines will lengthen to five years — from 180 days — the amount of time the center can retain private information about Americans when there is no suspicion that they are tied to terrorism, intelligence officials said. The guidelines are also expected to result in the center making more copies of entire databases and "data mining them" using complex algorithms to search for patterns that could indicate a threat.

Intelligence officials on Thursday said the new rules have been under development for about 18 months, and grew out of reviews launched after the failure to connect the dots about Umar Farouk Abdulmutallab, the "underwear bomber," before his Dec. 25, 2009, attempt to bomb a Detroit-bound airliner.

After the failed attack, government agencies discovered they had intercepted communications by Al Qaeda in the Arabian Peninsula and received a report from a United States Consulate in Nigeria that could have identified the attacker, if the information had been compiled ahead of time.

The changes are intended to allow analysts to more quickly identify terrorism suspects. But they also set off civil-liberties concerns among privacy advocates who invoked the "Total Information Awareness" program. That program, proposed early in the George W. Bush administration and partially shut down by Congress after an outcry, proposed fusing vast archives of electronic records — like travel records, credit card transactions, phone calls and more — and searching for patterns of a hidden terrorist cell.

Palentir

But national security officials stressed that analysts could already get the same information under the old rules, just in a more cumbersome way. They cited safeguards to protect against abuse, including audits of searches. The same rules apply to access by other federal agencies involved in counterterrorism.

“There is a genuine operational need to try to get us into a position where we can make the maximum use of the information the government already has to protect people,” said Robert S. Litt, the general counsel in the office of the Director of National Intelligence, which oversees the National Counterterrorism Center. “We have to manage to do that in a way that provides protection to people’s civil liberties and privacy. And I really think this has been a good-faith and reasonably successful effort to do that.”

The center has developed a priority list of databases it wants to copy entirely, but he and other officials declined to say which ones they were. (The Department of Homeland Security says it has already shared several entire databases, including records related to refugees, foreign students and international travelers.)

“We’re all in the dark, and for all we know it could be a rerun of Total Information Awareness, which would have allowed the government to make a computerized database of everything on everybody,” said Kate Martin, the director of the Center for National Security Studies, who criticized the administration for not making the draft guidelines public for scrutiny ahead of time.

The guidelines were also signed by the director of national intelligence, James R. Clapper Jr., and the director of the center, Matthew G. Olsen.

The previous guidelines for sharing information with the counterterrorism center were issued by Attorney General Michael Mukasey in 2008.

They set up three tracks by which the center could retrieve information gathered by another agency: by doing a limited search itself for certain data, by asking another agency to perform such a search, or — in cases where neither was sufficient — by replicating the database and analyzing the information itself.

The new guidelines keep that structure in place, but put greater emphasis on the third track, while also relaxing restrictions on how long data on Americans who have no known tie to terrorism may be stored. The old guidelines said data on innocent Americans must be deleted promptly, which the agency interpreted to mean if no tie to terrorism was detected within 180 days.

The new guidelines are intended to allow the center to hold on to information about

Americans for up to five years, although the agencies that collected the information — and can negotiate about how it will be used — may place a shorter life span on it.

Moreover, the first two tracks for searching the databases that remain under the control of the original agencies prohibit “pattern analysis.” But that restriction does not apply to databases the center has copied.

Marc Rotenberg, executive director of the Electronic Privacy Information Center, voiced concerns about how the guidelines would interact with proposals to give the government greater access to telecommunications information in order to protect critical infrastructure from hackers.

The new rules are silent about the use of commercial data — like credit card and travel records — that may have been acquired by other agencies. In 2009, Wired Magazine obtained a list of databases acquired by the Federal Bureau of Investigation, one of the agencies that shares information with the center. It included nearly 200 million records transferred from private data brokers like ChoicePoint, 55,000 entries on customers of Wyndham hotels, and numerous other travel and commercial records.

Intelligence officials offered a hypothetical scenario to explain one way the change could be helpful: A person from Yemen applies for a visa and lists an American as a point of contact. There is no sign that either person is a terrorist. Two years later, another person from Yemen applies for a visa and lists the same American, and this second person is a suspected terrorist.

Under the existing system, they said, to discover that the first visa applicant now had a known tie to a suspected terrorist, an analyst would have to ask the State Department to check its database to see if the American’s name had come up on anyone else’s visa application — a step that could ~~be overlooked or~~ cause a delay. Under the new rules, a computer could instantly alert analysts of the connection.

OK API



Read 10/18
in class

MARCH 25, 2012 | BY TREVOR TIMM



New Counterterrorism Guidelines Gives Authorities Vast Access to Private Info of Innocent Americans

On Thursday, U.S. Attorney General Eric Holder signed expansive new guidelines for terrorism analysts, allowing the National Counter Terrorism Center (NCTC) to mirror entire federal databases containing personal information and hold onto the information for an extended period of time—even if the person is not suspected of any involvement in terrorism. (Read the guidelines [here](#)).

Despite the “terrorism” justification, the new rules affect every single American. The agency now has free rein to, as the *New York Times*’ Charlie Savage put it, “retrieve, store and search information about Americans gathered by government agencies for purposes other than national security threats” and expands the amount of time the government can keep private information on *innocent individuals by a factor of ten*.

From the *New York Times*:

The guidelines will lengthen to five years — from 180 days — the amount of time the center can retain private information about Americans when there is no suspicion that they are tied to terrorism, intelligence officials said. The guidelines are also expected to result in the center making more copies of entire databases and “data mining them” using complex algorithms to search for patterns that could indicate a threat. (emphasis ours)

Journalist Marcy Wheeler summed the new guidelines up nicely saying, “So...the data the government keeps to track our travel, our taxes, our benefits, our identity? It just got transformed from bureaucratic data into national security intelligence.”

The administration claims that the changes in the rules for the NCTC—as well as for the Office of the Director of National Intelligence (DNI), which oversees the nation’s intelligence agencies—are in response to the government’s failure to connect the dots in the so-called “underwear bomber” case at the end of 2009, yet there was no explanation of how holding onto innocent Americans’ private data for five years would have stopped the bombing attempt.

Disturbingly, “oversight” for these expansive new guidelines is being directed by the DNI’s “Civil Liberties Protection Officer” Joel Alexander, who is so concerned about Americans’ privacy and civil liberties that he, as Marcy Wheeler notes, found no civil liberties concerns with the National Security Agency’s illegal warrantless wiretapping program when he reviewed it during President George W. Bush’s administration.

As other civil liberties organizations have noted, the new guidelines are reminiscent of the Orwellian-sounding “Total Information Awareness” program George Bush tried but failed to get through Congress in 2003—again in the name of defending the nation from terrorists. The program, as the *New York Times* explained, sparked an “outcry” and partially shut down Congress because it “proposed fusing vast archives of electronic records — like travel records, credit card transactions, phone calls and more — and searching for patterns of a hidden terrorist cell.”

SEARCH

Donate to EFF

Stay in Touch

Email Address

Zip Code (optional)

SIGN UP NOW

Follow EFF

Advertisers' assault on online #privacy continues. Here's where we draw the line: <https://eff.org/r.4an5> #DNTrack
OCT 12 @ 4:42PM

Chevron demands email providers turn over account info on environmental crusaders. <https://eff.org/r.5an3> @EFF & @EarthRightsIntl are on it.
OCT 12 @ 1:42PM

Twitter Facebook Identi.ca

Projects

HTTPS Everywhere

Bloggers' Rights

Coders' Rights

FOIA Project

Follow EFF

Free Speech Weak Links

Global Chokepoints

Patent Busting

Surveillance Self-Defense

Takedown Hall of Shame

Teaching Copyright

Ways To Help

The *New York Times* reported, the new NCTC guidelines “are silent about the use of commercial data — like credit card and travel records — that may have been acquired by other agencies,” but information first obtained by private corporations has ended up in federal databases before. In one example, *Wired Magazine* found FBI databases contained “200 million records transferred from private data brokers like ChoicePoint, 55,000 entries on customers of Wyndham hotels, and numerous other travel and commercial records.” The FBI would be one of the agencies sharing intelligence with the NCTC.

Despite Congress’ utter rejection of the “Total Information Awareness” program (TIA) in 2003, this is the second time this month the administration has been accused of instituting the program piecemeal. In his detailed report on the NSA’s new “data center” in Utah, *Wired Magazine*’s James Bamford remarked that the new data storage complex is “the realization” of the TIA program, as it’s expected to store and catalog “all forms of communication, including the complete contents of private emails, cell phone calls, and Google searches.”

Unfortunately, the new NCTC guidelines are yet another example of the government using the word “terrorism” to infringe on the rights of innocent Americans. Aside from the NSA’s aforementioned warrantless wiretapping program, we have seen the Patriot Act overwhelmingly used in criminal investigations *not* involving terrorism, despite its original stated purpose. As PBS Frontline’s Azmat Khan noted in response to the new guidelines, investigative journalist Dana Priest has previously reported how “many states have yet to use their vast and growing anti-terror apparatus to capture any terrorists; instead the government has built a massive database that collects, stores and analyzes information on thousands of U.S. citizens and residents, many of whom have not been accused of any wrongdoing.”

This problem has been well documented for years, yet Congress and both the Bush and Obama administrations have continued to use terrorism as a justification for expansive laws, and Americans’ constitutional rights have become collateral damage.

Privacy

MORE DEEPLINKS POSTS LIKE THIS

- OCTOBER 2012
New Senate Report: Counterterrorism "Fusion Centers" Invade Innocent Americans' Privacy and Don't Stop Terrorism
- DECEMBER 2004
9/11 Legislation Launches Misguided Data-Mining and Domestic Surveillance Schemes
- AUGUST 2008
Public Pressure Mounts Against Invasive Border Searches
- OCTOBER 2011
Ten Years After the Patriot Act, a Look at Three of the Most Dangerous Provisions Affecting Ordinary Americans
- APRIL 2012
CISPA, "National Security," and the NSA's Ability to Read Your Emails

RECENT DEEPLINKS POSTS

- OCT 12, 2012
Ad Industry's Assault on "Do Not Track" Continues at the W3C Amsterdam Meeting
- OCT 10, 2012
The Fight Against Data Retention Mandates In Slovakia
- OCT 10, 2012
Digitizing Books Is Fair Use: Author's Guild v. HathiTrust
- OCT 10, 2012
Canada Joins TPP as a Second-Tier Negotiator: Entertainment Lobby Approves, Civil Society Does Not
- OCT 10, 2012
EFF Opposes US Government's State Secrets Claim (Again) in Jewel v. NSA, the Warrantless Wiretapping Case

DEEPLINKS TOPICS

- | | | |
|-------------------------------------|-------------------------|-----------------|
| Analog Hole | Encrypting the Web | PATRIOT Act |
| Anonymity | Export Controls | Pen Trap |
| Anti-Counterfeiting Trade Agreement | FAQs for Lodsys Targets | Policy Analysis |

Biometrics	File Sharing	Printers
Bloggers Under Fire	FOIA	Privacy
Bloggers' Rights	Free Speech	Reading Accessibility
Broadcast Flag	FTAA	Real ID
Broadcasting Treaty	Hollywood v. DVD	RFID
CALEA	How Patents Hinder Innovation (Graphic)	Search Engines
CDA 230	Innovation	Search Incident to Arrest
Cell Tracking	Intellectual Property	Section 230 of the Communications Decency Act
Coders' Rights Project	International	Security
Content Blocking	International Privacy Standards	Social Networks
Copyright Trolls	Internet Governance Forum	SOPA/PIPA: Internet Blacklist Legislation
Council of Europe	Locational Privacy	State -sponsored malware
Cyber Security Legislation CISPA, SECURE IT, Cybersecurity Act	Mandatory Data Retention	Surveillance Drones
CyberSLAPP	Mandatory National IDs and Biometric Databases	Terms Of (Ab)Use
Development Agenda	Mass Surveillance Technologies	Test Your ISP
Digital Books	National Security Letters	The Global Network Initiative
Digital Radio	Net Neutrality	Trans Pacific Partnership Agreement
Digital Video	No Downtime for Free Speech	Transparency
DMCA	NSA Spying	Travel Screening
DMCA Rulemaking	OECD	Trusted Computing
Do Not Track	Online Behavioral Tracking	Uncategorized
DRM	Open Wireless	Video Games
E-Voting Rights	Patent Busting Project	Wikileaks
EFF Europe	Patent Trolls	WIPO
EFF Software Projects	Patents	Broadcast Flag



Hal is now calling on people

Net Neutrality:

Grades up

Good on substance

Complicated procedural posture

Hard: Understanding situation + audience
for super busy

Concise

Summarize

boil down complexity

pt summary up front

recommendations

headings, bold, underline

Short sentences

be good advocates

②

Don't have to take their arguments

Cavileer about new laws

↳ Why hard

What to get done

(Never read stellar comments)

Just tell us

Not "I'll tell ya"

Not just platonic ideals

Evolution of 1st Amendment

Next week: Commercial privacy

Sign

I killed
Paul

← messy handwriting
Encoded

(reasonable expectation of privacy?)

③ (Hal's Michael is pretty contrarian)

He's trying to defend

1. Subjectively they thought right to privacy
2. Does society feel that expectation is reasonable

intrusion in protected area
or reasonable area

is the search reasonable?
(not reasonableness of expectations!)
of privacy

Garbage cans

bright line rule → Once item in garbage can
can be close or far (behind house)
(on street)

Courts try to be clear to police

(4)

garbage - expected to take away

public vs private

What

very simple one

but what do you do w/ your trash?

DNA- etc

Shredded material

is that privacy

Will there be a revolution in surveillance?

Smith v Maryland

Pen register

Since it's recorded at phone company

5

How do courts decide what citizens view?
Survey - No
explain some things
Operator assisted call

Us vs Miller

Bank records

between you and bank teller
lots of security

is voluntariness important?

What must gov do?

Get subpoena - from prosecutors

What is a search?

Not if exposed to 3rd party

And 3rd party holding it counts as exposed

(6)

Kylao Thermal Imaging Camera

Justin Scelia

On the right

Originalist

250 much more narrow

new tech

allowing intrusion

otherwise not possible

but any person can fly over home

& take pictures

is thermal imaging common

you lived enough w/ airplanes

entirely possible look at window

but thermal imaging is rare

⑦

So in 10 years when thermal imaging is common?

Does Scalia like expectation argument?

What can you see w/ or w/o a physical search?

Mostly concerned is the home intruded on?

not really concerned w/ how

or expectations of homeowners ~~the~~

bright line test

~~the~~

based what is already observable

Dissent

hearth was visible outside house

Through the wall vs off the wall

act of sensing does not actually get inside

Could tell by how fast snow melts on the roof

8
Scala → nothing about expectations

Court does not do surveys

if big fans + might be intentionally exposing
have no expectation of privacy

Need bright line rule for police

Inferences — are they a search?

an inference is not a search
not viewing private details
just generalization

Mangard and Jones case

One was an appeal for Jones
diff set of arguments

⑨
knots - had to follow it closely

What was Jones's expectation of privacy?

- traveling in public so people could track his tracks

- but how is it different doing it for a month!

Objective Prong 1: Society does not expect
someone follows him on any trip

Prong 2: Society does not expect

Mosaic details - combining each indiv legal

surveillance you get level of surveillance

Society feels too intrusive

so it becomes a search

Surprising when they went for the mosaic theory
not a ~~well~~ common theory

(10)

Scalia discards expectations
back to the gov is trespassing
placing the GPS

Like camera on pizza box

Scalia doesn't care about duration

Vote 5-4

disagreement on which argument
trespass

reasonable expectation of privacy

Alito: trespassing view is obsolete

Sotomayor: (missed)

3rd party records are in Smith

①①

Give data to 3rd parties for convenience purposes

Alito: It's really how GPS data is used

Scalia is focusing on something far narrower

Will be able to co-op ~~the~~ GPS built into car

Smith vs Maryland Dissent

Thurgood Marshall

(no one read it)

Prof: you should

~~The~~ Digital Due Process

Protecting email on survey

How would you write a law?

Last weeks Wilber-Hale memo

(12)

Higher standards for gov access to this data
Email stored in cloud diff
> 180 days diff

Cellphone location records
Kyab → fairly unprotected
info stored on network

Google Search History
Under what standards
Warrant
or Suppencia

But Law Enforcement does not want less power
And political leaders very sensitive to
ammo against Dem in the election

(12)

Strong desire to not be weak on crime

Used to be civil liberties block

both parties

but

Why ~~was~~ was Manard appealed?

~~Now~~ Solicitor General

Law Enforcement has a view

not considered a political decision

if Appeal \rightarrow risky

Did Gov win or lose?

Was a circuit split

2 circuits disagree

One reason \rightarrow can't have diff rules
across the country

(most people didn't vote)

(13)

Suprem Court will need to decide again

Very small people to fight for this law
Took years to put this collation does it

(missed)

↳ lots of questions
cell phone records
etc

This case could have added clarity,
but no

Change is a big risk
big institutional interests

telling law enforcement things should be diff-
lots of people in DC are worry about
risk of changing things

(14)

So must answer why your change is not only good, but unthreatening

(Break)

Group Projects

Next week outline

ideas clear by then

Who are you writing it for

do they need by i

for public i

Must think about that

identify who memo is too

Will be asked to comment on others work
including today

15

Upper 3rd Party data
for FTC

what ~~an~~ cos should do when get
gov request

eff report → who has your back
from ~~DATA~~ EFF

FTC vs DOJ?

Interagency Committee on privacy

GNI - Global Network Initiative

Internet Governance

(missed)

Who could write a memo to the President?

Cab-level secretary

Or head of one of the Councils?

(16)

UAV

Congress required FAA not to regulate hobby aircraft

Is it diff if it's a hobby?

Lots of very specific state rules

Offensive Cyber Attacks

White House

David Eddleman

lots of subterfuge

but less than meets the eye

Textbooks

monopolistic

authors can't release books for free

Prof, not just hand winging
positive recommendation

(17)

Think about what goal ya have
What to target/avoid
Inventory of possible steps

Copyright

(missed)

ad networks

SOPA

opposition

what legislation to success

address main opposition

Target: Intellectual Property Coordinators
Just looks at enforcement

or National Economic Council

don't write what happened w/ SOPA

(18)

Cloud Based email

For Mobile data privacy

Greg NoJan
Esp

Senate Judiciary Subcommittee

Circumvention

How effective is funding of Tor?

White House target

Privacy Delinking

Non personally identifiable

Prof: hard but falsed

Copyright (us)

Target Audience: Bad

Impa

(19)

Similar and i ~~best~~

National Economic Council

Still no mentor

ASAP

How much economic analysis?

Economist

decide what mean

We're behind

Study - Post HADOPT

Reactions

Int Photographic

Small grp of economists lot of work
augment

①

Policy direction want to develop

the "hadoop" economic study"
Wiki with a lot of studies
not complete

Framework

not purely economic
does it have an effect

Diff things from diff prot

Then start more fleshed out list of what
framework items look like

Methodology:

How will answer q?

② What is model/methodology to use for test

World - diff eq

↳ not what planning

lots of people in econ

What mentor tell ya about?

DC policy space

music industry

Who would use it?

What ans they ~~all~~ get?

Principles in guide policy makers

How measure againsts principles

Objective principles

Pseudo optimal

(22)

Fewer of bad tradeoffs

Could infer framework from last 4 years

- not much legislation
 - aggressive enforcement
 - industry vol best practices
-
- cut down on piracy
 - no big legislation

What ended up happening

Take a shot on outline

Wild ass guess on what in framework

CCIA Fair Use Economy Study

6.805 Class 8, Oct 25: Privacy Law in the US

Class 8, Oct 25: 2012 - Consumer Privacy Protection in the US6.805: Foundations of Internet Policy - Semester Calendar

Meets in 36-156

Read 10/31
Super late**Assignment due Oct. 24 (on Stellar, one paper per team)**

Each team should turn in a complete outline of your report. By complete outline, we mean that you should present the major conclusions of your report and the logic that leads to them. This does not have to be written in polished English, and it can even be in outline form. But it should cover the major content of your report: What you're recommending and how you will support those recommendations.

In particular, it should cover:

- Who is the report addressed to?
- What's the problem?
- What are possible solutions?
- Why is our solution better than other solutions?
- What are arguments against our solution and how do you respond to them?
- Proposed bibliography

To help you get oriented, here are some guidelines on writing policy papers. (These pertain to the final paper, not to this draft.)

This week's class**Goals**

This week's class discusses consumer data privacy law in the US, where policy is being increasingly challenged by technology advances in cloud storage and data mining. As with last week, there is a lot of material, but please try to master it.

What is privacy?

- 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data
- Daniel Solove, A Taxonomy of Privacy, *Univ. Pennsylvania Law Review*, January 2006. (read carefully pp 477-491 and skim the rest)

No one knows what privacy is

State of US law and enforcement actions

Federal Trade Commission statutory authority and enforcement actions

- Federal Trade Commission Act Section 5, as codified at 15 USC 45 [read Section (a)]

FTC Enforcement actions

- *In the Matter of Sears Holdings Management Company*, Complaint and Order.
- *In the Matter of Google Inc.*, EPIC complaint, Complaint, Order.

European Union Privacy Enforcement

- French Data Protection CNIL action on Google Privacy Policy (October 2012)
- Google: Let us opt out of your data mining machine, *Wired*, Oct. 17, 2012.

New Policy Frameworks

- White House, Consumer Data Privacy in a Networked World (Feb. 2012)
- Federal Trade Commission, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers (March 2012)
- Bamberger and Mulligan, Privacy on the Books and on the Ground, *Stanford Law Review* Vol. 63, January 2011 (concentrate on pp. 249-270, 295-311)
- Some of the libertarian perspectives on privacy at the Technology Liberation Front. (See, e.g., "White House Ignores Real Bill of Rights in Call for Privacy Regulation of Internet Businesses.")

Class Activity

The last hour of the class will be a group activity where you'll be asked to formulate responses to last week's CNIL's actions against Google, from the following groups:

1. Google as a company
2. Internet advertising industry as a whole
3. Facebook, Twitter, Apple
4. Progressive privacy advocates
5. Conservative/libertarian privacy advocates
6. US Congress
7. White House

Published by Google Docs – Report Abuse – Updated automatically every 5 minutes

Read 10/31

[OECD Home](#) » [Internet](#) » [Internet economy](#) » [OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data](#)

Internet economy

Broadband and telecom

Internet economy

Consumer policy

Public sector innovation and
e-government

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data

[Send](#) [Print](#) [Tweet](#)

[Background](#)

[Preface](#)

[OECD Council Recommendation](#)

[Guidelines](#)

- [Part 1. General definitions](#)
- [Part 2. Basic principles of national application](#)
- [Part 3. Basic principles of international application: Free flow and legitimate restrictions](#)
- [Part 4. National implementation](#)
- [Part 5. International co-operation](#)

[Explanatory Memorandum](#)

- [Introduction](#)
- [General background: The problems | Activities at national level | International aspects of privacy and data banks | Relevant international activities | Activities of the OECD](#)
- [The Guidelines: Purpose and scope | Detailed comments | Follow-up](#)

Preface

The development of automatic data processing, which enables vast quantities of data to be transmitted within seconds across national frontiers, and indeed across continents, has made it necessary to consider privacy protection in relation to personal data. Privacy protection laws have been introduced, or will be introduced shortly, in approximately one half of OECD Member countries (Austria, Canada, Denmark, France, Germany, Luxembourg, Norway, Sweden and the United States have passed legislation. Belgium, Iceland, the Netherlands, Spain and Switzerland have prepared draft bills) to prevent what are considered to be violations of fundamental human rights, such as the unlawful storage of personal data, the storage of inaccurate personal data, or the abuse or unauthorised disclosure of such data.

On the other hand, there is a danger that disparities in national legislations could hamper the free flow of personal data across frontiers; these flows have greatly increased in recent years and are bound to grow further with the widespread introduction of new computer and communications technology. Restrictions on these flows could cause serious disruption in important sectors of the economy, such as banking and insurance.

For this reason, OECD Member countries considered it necessary to develop Guidelines which would help to harmonise national privacy legislation and, while upholding such human rights, would at the same time prevent interruptions in international flows of data. They represent a consensus on basic principles which can be built into existing national legislation, or serve as a basis for legislation in those countries which do not yet have it.

The Guidelines, in the form of a Recommendation by the Council of the OECD, were developed by a group of government experts under the chairmanship of The Hon. Mr. Justice M.D. Kirby, Chairman of the Australian Law Reform Commission. The Recommendation was adopted and became applicable on 23 September 1980.

The Guidelines are accompanied by an Explanatory Memorandum intended to provide information on the discussion and reasoning underlining their formulation.

1980!

OECD Council Recommendation

RECOMMENDATION OF THE COUNCIL CONCERNING GUIDELINES GOVERNING THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA (23 September 1980)

THE COUNCIL,

Having regard to articles 1(c), 3(a) and 5(b) of the Convention on the Organisation for Economic Co-operation and

Development of 14th December, 1960;

RECOGNISING:

- that, although national laws and policies may differ, Member countries have a common interest in protecting privacy and individual liberties, and in reconciling fundamental but competing values such as privacy and the free flow of information;
- that automatic processing and transborder flows of personal data create new forms of relationships among countries and require the development of compatible rules and practices;
- that transborder flows of personal data contribute to economic and social development;
- that domestic legislation concerning privacy protection and transborder flows of personal data may hinder such transborder flows;

Determined to advance the free flow of information between Member countries and to avoid the creation of unjustified obstacles to the development of economic and social relations among Member countries;

RECOMMENDS:

- that Member countries take into account in their domestic legislation the principles concerning the protection of privacy and individual liberties set forth in the Guidelines contained in the Annex to this Recommendation which is an integral part thereof;
- that Member countries endeavour to remove or avoid creating, in the name of privacy protection, unjustified obstacles to transborder flows of personal data;
- that Member countries co-operate in the implementation of the Guidelines set forth in the Annex;
- that Member countries agree as soon as possible on specific procedures of consultation and co-operation for the application of these Guidelines.

[\(back to top of page\)](#)

Annex to the Recommendation of the Council of 23rd September 1980:

GUIDELINES GOVERNING THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA

PART ONE. GENERAL DEFINITIONS

1. For the purposes of these Guidelines:

- a) "data controller" means a party who, according to domestic law, is competent to decide about the contents and use of personal data regardless of whether or not such data are collected, stored, processed or disseminated by that party or by an agent on its behalf;
- b) "personal data" means any information relating to an identified or identifiable individual (data subject);
- c) "transborder flows of personal data" means movements of personal data across national borders.

Scope of the Guidelines

2. These Guidelines apply to personal data, whether in the public or private sectors, which, because of the manner in which they are processed, or because of their nature or the context in which they are used, pose a danger to privacy and individual liberties.

3. These Guidelines should not be interpreted as preventing:

- a) the application, to different categories of personal data, of different protective measures depending upon their nature and the context in which they are collected, stored, processed or disseminated;
- b) the exclusion from the application of the Guidelines of personal data which obviously do not contain any risk to privacy and individual liberties; or
- c) the application of the Guidelines only to automatic processing of personal data.

4. Exceptions to the Principles contained in Parts Two and Three of these Guidelines, including those relating to national sovereignty, national security and public policy ("ordre public"), should be:

- a) as few as possible, and
- b) made known to the public.

5. In the particular case of Federal countries the observance of these Guidelines may be affected by the division of powers in the Federation.

6. These Guidelines should be regarded as minimum standards which are capable of being supplemented by additional measures for the protection of privacy and individual liberties.

[\(back to top of page\)](#)

PART TWO. BASIC PRINCIPLES OF NATIONAL APPLICATION

Collection Limitation Principle

7. There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

Data Quality Principle

8. Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

Purpose Specification Principle

9. The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

Use Limitation Principle

10. Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except:

- a) with the consent of the data subject; or
- b) by the authority of law.

Security Safeguards Principle

11. Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.

Openness Principle

12. There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

Individual Participation Principle

13. An individual should have the right:

- a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;
- b) to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him;
- c) to be given reasons if a request made under subparagraphs(a) and (b) is denied, and to be able to challenge such denial; and
- d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

Accountability Principle

14. A data controller should be accountable for complying with measures which give effect to the principles stated above.

[\(back to top of page\)](#)

PART THREE. BASIC PRINCIPLES OF INTERNATIONAL APPLICATION: FREE FLOW AND LEGITIMATE RESTRICTIONS

15. Member countries should take into consideration the implications for other Member countries of domestic processing and re-export of personal data.

16. Member countries should take all reasonable and appropriate steps to ensure that transborder flows of personal data, including transit through a Member country, are uninterrupted and secure.

17. A Member country should refrain from restricting transborder flows of personal data between itself and another Member country except where the latter does not yet substantially observe these Guidelines or where the re-export of such data would circumvent its domestic privacy legislation. A Member country may also impose restrictions in respect of certain categories of personal data for which its domestic privacy legislation includes specific regulations in view of the nature of those data and for which the other Member country provides no equivalent protection.

18. Member countries should avoid developing laws, policies and practices in the name of the protection of privacy and individual liberties, which would create obstacles to transborder flows of personal data that would exceed requirements for such protection.

[\(back to top of page\)](#)

PART FOUR. NATIONAL IMPLEMENTATION

19. In implementing domestically the principles set forth in Parts Two and Three, Member countries should establish legal, administrative or other procedures or institutions for the protection of privacy and individual liberties in respect of personal data. Member countries should in particular endeavour to:

- a) adopt appropriate domestic legislation;
- b) encourage and support self-regulation, whether in the form of codes of conduct or otherwise;

- c) provide for reasonable means for individuals to exercise their rights;
- d) provide for adequate sanctions and remedies in case of failures to comply with measures which implement the principles set forth in Parts Two and Three; and
- e) ensure that there is no unfair discrimination against data subjects.

[\(back to top of page\)](#)

PART FIVE. INTERNATIONAL CO-OPERATION

20. Member countries should, where requested, make known to other Member countries details of the observance of the principles set forth in these Guidelines. Member countries should also ensure that procedures for transborder flows of personal data and for the protection of privacy and individual liberties are simple and compatible with those of other Member countries which comply with these Guidelines.

21. Member countries should establish procedures to facilitate:

information exchange related to these Guidelines, and

mutual assistance in the procedural and investigative matters involved.

22. Member countries should work towards the development of principles, domestic and international, to govern the applicable law in the case of transborder flows of personal data.

[\(back to top of page\)](#)

EXPLANATORY MEMORANDUM

INTRODUCTION

A feature of OECD Member countries over the past decade has been the development of laws for the protection of privacy. These laws have tended to assume different forms in different countries, and in many countries are still in the process of being developed. The disparities in legislation may create obstacles to the free flow of information between countries. Such flows have greatly increased in recent years and are bound to continue to grow as a result of the introduction of new computer and communication technology.

The OECD, which had been active in this field for some years past, decided to address the problems of diverging national legislation and in 1978 instructed a Group of Experts to develop Guidelines on basic rules governing the transborder flow and the protection of personal data and privacy, in order to facilitate the harmonization of national legislation. The Group has now completed its work.

The Guidelines are broad in nature and reflect the debate and legislative work which has been going on for several years in Member countries. The Expert Group which prepared the Guidelines has considered it essential to issue an accompanying Explanatory Memorandum. Its purpose is to explain and elaborate the Guidelines and the basic problems of protection of privacy and individual liberties. It draws attention to key issues that have emerged in the discussion of the Guidelines and spells out the reasons for the choice of particular solutions.

The first part of the Memorandum provides general background information on the area of concern as perceived in Member countries. It explains the need for international action and summarises the work carried out so far by the OECD and certain other international organisations. It concludes with a list of the main problems encountered by the Expert Group in its work.

Part Two has two subsections. The first contains comments on certain general features of the Guidelines, the second detailed comments on individual paragraphs.

This Memorandum is an information document, prepared to explain and describe generally the work of the Expert Group. It is subordinate to the Guidelines themselves. It cannot vary the meaning of the Guidelines but is supplied to help in their interpretation and application.

[\(back to top of page\)](#)

I. GENERAL BACKGROUND

The problems

1. The 1970s may be described as a period of intensified investigative and legislative activities concerning the protection of privacy with respect to the collection and use of personal data. Numerous official reports show that the problems are taken seriously at the political level and at the same time that the task of balancing opposing interests is delicate and unlikely to be accomplished once and for all. Public interest has tended to focus on the risks and implications associated with the computerised processing of personal data and some countries have chosen to enact statutes which deal exclusively with computers and computer-supported activities. Other countries have preferred a more general approach to privacy protection issues irrespective of the particular data processing technology involved.

2. The remedies under discussion are principally safeguards for the individual which will prevent an invasion of privacy in the classical sense, i.e. abuse or disclosure of intimate personal data; but other, more or less closely related needs for protection have become apparent. Obligations of record-keepers to inform the general public about activities concerned with the processing of data, and rights of data subjects to have data relating to them supplemented or amended, are two random examples. Generally speaking, there has been a tendency to broaden the traditional concept of privacy ("the right to be left alone") and to identify a more complex synthesis of interests which can perhaps more correctly be termed privacy and individual liberties.

3. As far as the legal problems of automatic data processing (ADP) are concerned, the protection of privacy and individual liberties constitutes perhaps the most widely debated aspect. Among the reasons for such widespread concern are the ubiquitous use of computers for the processing of personal data, vastly expanded possibilities of storing, comparing, linking, selecting and accessing personal data, and the combination of computers and telecommunications technology which may place personal data simultaneously at the disposal of thousands of users at geographically dispersed locations and enables the pooling of data and the creation of complex national and international data networks. Certain problems require particularly urgent attention, e.g. those relating to emerging international data networks, and to the need of balancing competing interests of privacy on the one hand and freedom of information on the other, in order to allow a full exploitation of the potentialities of modern data processing technologies in so far as this is desirable.

[\(back to top of page\)](#)

Activities at national level

4. Of the OECD Member countries more than one-third have so far enacted one or several laws which, among other things, are intended to protect individuals against abuse of data relating to them and to give them the right of access to data with a view to checking their accuracy and appropriateness. In federal states, laws of this kind may be found both at the national and at the state or provincial level. Such laws are referred to differently in different countries. Thus, it is common practice in continental Europe to talk about "data laws" or "data protection laws" (*lois sur la protection des données*), whereas in English speaking countries they are usually known as "privacy protection laws". Most of the statutes were enacted after 1973 and this present period may be described as one of continued or even widened legislative activity. Countries which already have statutes in force are turning to new areas of protection or are engaged in revising or complementing existing statutes. Several other countries are entering the area and have bills pending or are studying the problems with a view to preparing legislation. These national efforts, and not least the extensive reports and research papers prepared by public committees or similar bodies, help to clarify the problems and the advantages and implications of various solutions. At the present stage, they provide a solid basis for international action.

5. The approaches to protection of privacy and individual liberties adopted by the various countries have many common features. Thus, it is possible to identify certain basic interests or values which are commonly considered to be elementary components of the area of protection. Some core principles of this type are: setting limits to the collection of personal data in accordance with the objectives of the data collector and similar criteria; restricting the usage of data to conform with openly specified purposes; creating facilities for individuals to learn of the existence and contents of data and have data corrected; and the identification of parties who are responsible for compliance with the relevant privacy protection rules and decisions. Generally speaking, statutes to protect privacy and individual liberties in relation to personal data attempt to cover the successive stages of the cycle beginning with the initial collection of data and ending with erasure or similar measures, and to ensure to the greatest possible extent individual awareness, participation and control.

6. Differences between national approaches as apparent at present in laws, bills or proposals for legislation refer to aspects such as the scope of legislation, the emphasis placed on different elements of protection, the detailed implementation of the broad principles indicated above, and the machinery of enforcement. Thus, opinions vary with respect to licensing requirements and control mechanisms in the form of special supervisory bodies ("data inspection authorities"). Categories of sensitive data are defined differently, the means of ensuring openness and individual participation vary, to give just a few instances. Of course, existing traditional differences between legal systems are a cause of disparity, both with respect to legislative approaches and the detailed formulation of the regulatory framework for personal data protection.

[\(back to top of page\)](#)

International aspects of privacy and data banks

7. For a number of reasons the problems of developing safeguards for the individual in respect of the handling of personal data cannot be solved exclusively at the national level. The tremendous increase in data flows across national borders and the creation of international data banks (collections of data intended for retrieval and other purposes) have highlighted the need for concerted national action and at the same time support arguments in favour of free flows of information which must often be balanced against requirements for data protection and for restrictions on their collection, processing and dissemination.

8. One basic concern at the international level is for consensus on the fundamental principles on which protection of the individual must be based. Such a consensus would obviate or diminish reasons for regulating the export of data and facilitate resolving problems of conflict of laws. Moreover, it could constitute a first step towards the development of more detailed, binding international agreements.

9. There are other reasons why the regulation of the processing of personal data should be considered in an international context: the principles involved concern values which many nations are anxious to uphold and see generally accepted; they may help to save costs in international data traffic; countries have a common interest in preventing the creation of locations where national regulations on data processing can easily be circumvented; indeed, in view of the international mobility of people, goods and commercial and scientific activities, commonly accepted practices with regard to the processing of data may be advantageous even where no transborder data traffic is directly involved.

[\(back to top of page\)](#)

Relevant international activities

10. There are several international agreements on various aspects of telecommunications which, while facilitating relations

and co-operation between countries, recognise the sovereign right of each country to regulate its own telecommunications (The International Telecommunications Convention of 1973). The protection of computer data and programmes has been investigated by, among others, the World Intellectual Property Organisation which has developed draft model provisions for national laws on the protection of computer software. Specialised agreements aiming at informational co-operation may be found in a number of areas, such as law enforcement, health services, statistics and judicial services (e.g. with regard to the taking of evidence).

11. A number of international agreements deal in a more general way with the issues which are at present under discussion, viz. the protection of privacy and the free dissemination of information. They include the European Convention of Human Rights of 4th November, 1950 and the International Covenant on Civil and Political Rights (United Nations, 19th December, 1966).

12. However, in view of the inadequacy of existing international instruments relating to the processing of data and individual rights, a number of international organisations have carried out detailed studies of the problems involved in order to find more satisfactory solutions.

13. In 1973 and 1974 the Committee of Ministers of the Council of Europe adopted two resolutions concerning the protection of the privacy of individuals vis-à-vis electronic data banks in the private and public sectors respectively. Both resolutions recommend that the governments of the Member states of the Council of Europe take steps to give effect to a number of basic principles of protection relating to the obtaining of data, the quality of data, and the rights of individuals to be informed about data and data processing activities.

14. Subsequently the Council of Europe, on the instructions of its Committee of Ministers, began to prepare an international Convention on privacy protection in relation to data processing abroad and transfrontier data processing. It also initiated work on model regulations for medical data banks and rules of conduct for data processing professionals. The Convention was adopted by the Committee of Ministers on 17 September 1980. It seeks to establish basic principles of data protection to be enforced by Member countries, to reduce restrictions on transborder data flows between the Contracting Parties on the basis of reciprocity, to bring about co-operation between national data protection authorities, and to set up a Consultative Committee for the application and continuing development of the convention.

15. The European Community has carried out studies concerning the problems of harmonization of national legislations within the Community, in relation to transborder data flows and possible distortions of competition, the problems of data security and confidentiality, and the nature of transborder data flows. A sub-committee of the European Parliament held a public hearing on data processing and the rights of the individual in early 1978. Its work has resulted in a report to the European Parliament in spring 1979. The report, which was adopted by the European Parliament in May 1979, contains a resolution on the protection of the rights of the individual in the face of technical developments in data processing.

[\(back to top of page\)](#)

Activities of the OECD

16. The OECD programme on transborder data flows derives from computer utilisation studies in the public sector which were initiated in 1969. A Group of Experts, the Data Bank Panel, analysed and studied different aspects of the privacy issue, e.g. in relation to digital information, public administration, transborder data flows, and policy implications in general. In order to obtain evidence on the nature of the problems, the Data Bank Panel organised a Symposium in Vienna in 1977 which provided opinions and experience from a diversity of interests, including government, industry, users of international data communication networks, processing services, and interested intergovernmental organisations.

17. A number of guiding principles were elaborated in a general framework for possible international action. These principles recognised:

- a) the need for generally continuous and uninterrupted flows of information between countries,
- b) the legitimate interests of countries in preventing transfers of data which are dangerous to their security or contrary to their laws on public order and decency or which violate the rights of their citizens,
- c) the economic value of information and the importance of protecting "data trade" by accepted rules of fair competition,
- d) the needs for security safeguards to minimise violations of proprietary data and misuse of personal information, and
- e) the significance of a commitment of countries to a set of core principles for the protection of personal information.

18. Early in 1978 a new ad hoc Group of Experts on Transborder Data Barriers and Privacy Protection was set up within the OECD which was instructed to develop guidelines on basic rules governing the transborder flow and the protection of personal data and privacy, in order to facilitate a harmonization of national legislations, without this precluding at a later date the establishment of an international Convention. This work was to be carried out in close co-operation with the Council of Europe and the European Community and to be completed by 1 July 1979.

19. The Expert Group, under the chairmanship of the Honourable Mr. Justice Kirby, Australia, and with the assistance of Dr. Peter Seipel (Consultant), produced several drafts and discussed various reports containing, for instance, comparative analyses of different approaches to legislation in this field. It was particularly concerned with a number of key issues set out below.

- a) The specific, sensitive facts issue. The question arose as to whether the Guidelines should be of a general nature or whether they should be structured to deal with different types of data or activities (e.g. credit reporting).

Indeed, it is probably not possible to identify a set of data which are universally regarded as being sensitive.

- b) The ADP issue. The argument that ADP is the main cause for concern is doubtful and, indeed, contested.
- c) The legal persons issue. Some, but by no means all, national laws protect data relating to legal persons in a similar manner to data related to physical persons.
- d) The remedies and sanctions issue. The approaches to control mechanisms vary considerably: for instance, schemes involving supervision and licensing by specially constituted authorities might be compared to schemes involving voluntary compliance by record-keepers and reliance on traditional judicial remedies in the Courts.
- e) The basic machinery or implementation issue. The choice of core principles and their appropriate level of detail presents difficulties. For instance, the extent to which data security questions (protection of data against unauthorised interference, fire, and similar occurrences) should be regarded as part of the privacy protection complex is debatable; opinions may differ with regard to time limits for the retention, or requirements for the erasure, of data and the same applies to requirements that data be relevant to specific purposes. In particular, it is difficult to draw a clear dividing line between the level of basic principles or objectives and lower level "machinery" questions which should be left to domestic implementation.
- f) The choice of law issue. The problems of choice of jurisdiction, choice of applicable law and recognition of foreign judgements have proved to be complex in the context of transborder data flows. The question arose, however, whether and to what extent it should be attempted at this stage to put forward solutions in Guidelines of a non-binding nature.
- g) The exceptions issue. Similarly, opinions may vary on the question of exceptions. Are they required at all? If so, should particular categories of exceptions be provided for or should general limits to exceptions be formulated?
- h) The bias issue. Finally, there is an inherent conflict between the protection and the free transborder flow of personal data. Emphasis may be placed on one or the other, and interests in privacy protection may be difficult to distinguish from other interests relating to trade, culture, national sovereignty, and so forth.

20. During its work the Expert Group maintained close contacts with corresponding organs of the Council of Europe. Every effort was made to avoid unnecessary differences between the texts produced by the two organisations; thus, the set of basic principles of protection are in many respects similar. On the other hand, a number of differences do occur. To begin with, the OECD Guidelines are not legally binding, whereas the Council of Europe has produced a convention which will be legally binding among those countries which ratify it. This in turn means that the question of exceptions has been dealt with in greater detail by the Council of Europe. As for the area of application, the Council of Europe Convention deals primarily with the automatic processing of personal data whereas the OECD Guidelines apply to personal data which involve dangers to privacy and individual liberties, irrespective of the methods and machinery used in their handling. At the level of details, the basic principles of protection proposed by the two organisations are not identical and the terminology employed differs in some respects. The institutional framework for continued co-operation is treated in greater detail in the Council of Europe Convention than in the OECD Guidelines.

21. The Expert Group also maintained co-operation with the Commission of the European Communities as required by its mandate.

[\(back to top of page\)](#)

II. THE GUIDELINES

A. Purpose and Scope

General

22. The Preamble of the Recommendation expresses the basic concerns calling for action. The Recommendation affirms the commitment of Member countries to protect privacy and individual liberties and to respect the transborder flows of personal data.

23. The Guidelines set out in the Annex to the Recommendation consist of five parts. Part One contains a number of definitions and specifies the scope of the Guidelines, indicating that they represent minimum standards. Part Two contains eight basic principles (Paragraphs 7-14) relating to the protection of privacy and individual liberties at the national level. Part Three deals with principles of international application, i.e. principles which are chiefly concerned with relationships between Member countries.

24. Part Four deals, in general terms, with means of implementing the basic principles set out in the preceding parts and specifies that these principles should be applied in a non-discriminatory manner. Part Five concerns matters of mutual assistance between Member countries, chiefly through the exchange of information and by avoiding incompatible national procedures for the protection of personal data. It concludes with a reference to issues of applicable law which may arise when flows of personal data involve several Member countries.

Objectives

25. The core of the Guidelines consists of the principles set out in Part Two of the Annex. It is recommended to Member countries that they adhere to these principles with a view to:

- a) achieving acceptance by Member countries of certain minimum standards of protection of privacy and individual liberties with regard to personal data;
- b) reducing differences between relevant domestic rules and practices of Member countries to a minimum;
- c) ensuring that in protecting personal data they take into consideration the interests of other Member countries and the need to avoid undue interference with flows of personal data between Member countries; and

- d) eliminating, as far as possible, reasons which might induce Member countries to restrict transborder flows of personal data because of the possible risks associated with such flows.

As stated in the Preamble, two essential basic values are involved: the protection of privacy and individual liberties and the advancement of free flows of personal data. The Guidelines attempt to balance the two values against one another; while accepting certain restrictions to free transborder flows of personal data, they seek to reduce the need for such restrictions and thereby strengthen the notion of free information flows between countries.

26. Finally, Parts Four and Five of the Guidelines contain principles seeking to ensure:

- a) effective national measures for the protection of privacy and individual liberties;
- b) avoidance of practices involving unfair discrimination between individuals; and
- c) bases for continued international co-operation and compatible procedures in any regulation of transborder flows of personal data.

Level of detail

27. The level of detail of the Guidelines varies depending upon two main factors, viz. (a) the extent of consensus reached concerning the solutions put forward, and (b) available knowledge and experience pointing to solutions to be adopted at this stage. For instance, the Individual Participation Principle (Paragraph 13) deals specifically with various aspects of protecting an individual's interest, whereas the provision on problems of choice of law and related matters (Paragraph 22) merely states a starting-point for a gradual development of detailed common approaches and international agreements. On the whole, the Guidelines constitute a general framework for concerted actions by Member countries: objectives put forward by the Guidelines may be pursued in different ways, depending on the legal instruments and strategies preferred by Member countries for their implementation. To conclude, there is a need for a continuing review of the Guidelines, both by Member countries and the OECD. As and when experience is gained, it may prove desirable to develop and adjust the Guidelines accordingly.

Non-Member countries

28. The Recommendation is addressed to Member countries and this is reflected in several provisions which are expressly restricted to relationships between Member countries (see Paragraphs 15, 17 and 20 of the Guidelines). Widespread recognition of the Guidelines is, however, desirable and nothing in them should be interpreted as preventing the application of relevant provisions by Member countries to non-Member countries. In view of the increase in transborder data flows and the need to ensure concerted solutions, efforts will be made to bring the Guidelines to the attention of non-Member countries and appropriate international organisations.

The broader regulatory perspective

29. It has been pointed out earlier that the protection of privacy and individual liberties constitutes one of many overlapping legal aspects involved in the processing of data. The Guidelines constitute a new instrument, in addition to other, related international instruments governing such issues as human rights, telecommunications, international trade, copyright, and various information services. If the need arises, the principles set out in the Guidelines could be further developed within the framework of activities undertaken by the OECD in the area of information, computer and communications policies.

30. Some Member countries have emphasized the advantages of a binding international Convention with a broad coverage. The Mandate of the Expert Group required it to develop guidelines on basic rules governing the transborder flow and the protection of personal data and privacy, without this precluding at a later stage the establishment of an international Convention of a binding nature. The Guidelines could serve as a starting-point for the development of an international Convention when the need arises.

Legal persons, groups and similar entities

31. Some countries consider that the protection required for data relating to individuals may be similar in nature to the protection required for data relating to business enterprises, associations and groups which may or may not possess legal personality. The experience of a number of countries also shows that it is difficult to define clearly the dividing line between personal and non-personal data. For example, data relating to a small company may also concern its owner or owners and provide personal information of a more or less sensitive nature. In such instances it may be advisable to extend to corporate entities the protection offered by rules relating primarily to personal data.

32. Similarly, it is debatable to what extent people belonging to a particular group (i.e. mentally disabled persons, immigrants, ethnic minorities) need additional protection against the dissemination of information relating to that group.

33. On the other hand, the Guidelines reflect the view that the notions of individual integrity and privacy are in many respects particular and should not be treated the same way as the integrity of a group of persons, or corporate security and confidentiality. The needs for protection are different and so are the policy frameworks within which solutions have to be formulated and interests balanced against one another. Some members of the Expert Group suggested that the possibility of extending the Guidelines to legal persons (corporations, associations) should be provided for. This suggestion has not secured a sufficient consensus. The scope of the Guidelines is therefore confined to data relating to individuals and it is left to Member countries to draw dividing lines and decide policies with regard to corporations, groups and similar bodies (cf. paragraph 49 below).

Automated and non-automated data

34. In the past, OECD activities in privacy protection and related fields have focused on automatic data processing and

computer networks. The Expert Group has devoted special attention to the issue of whether or not these Guidelines should be restricted to the automatic and computer-assisted processing of personal data. Such an approach may be defended on a number of grounds, such as the particular dangers to individual privacy raised by automation and computerised data banks, and increasing dominance of automatic data processing methods, especially in transborder data flows, and the particular framework of information, computer and communications policies within which the Expert Group has set out to fulfil its Mandate.

35. On the other hand, it is the conclusion of the Expert Group that limiting the Guidelines to the automatic processing of personal data would have considerable drawbacks. To begin with, it is difficult, at the level of definitions, to make a clear distinction between the automatic and non-automatic handling of data. There are, for instance, "mixed" data processing systems, and there are stages in the processing of data which may or may not lead to automatic treatment. These difficulties tend to be further complicated by ongoing technological developments, such as the introduction of advanced semi-automated methods based on the use of microfilm, or microcomputers which may increasingly be used for private purposes that are both harmless and impossible to control. Moreover, by concentrating exclusively on computers the Guidelines might lead to inconsistency and lacunae, and opportunities for record-keepers to circumvent rules which implement the Guidelines by using non-automatic means for purposes which may be offensive.

36. Because of the difficulties mentioned, the Guidelines do not put forward a definition of "automatic data processing" although the concept is referred to in the preamble and in paragraph 3 of the Annex. It may be assumed that guidance for the interpretation of the concept can be obtained from sources such as standard technical vocabularies.

37. Above all, the principles for the protection of privacy and individual liberties expressed in the Guidelines are valid for the processing of data in general, irrespective of the particular technology employed. The Guidelines therefore apply to personal data in general or, more precisely, to personal data which, because of the manner in which they are processed, or because of their nature or context, pose a danger to privacy and individual liberties.

38. It should be noted, however, that the Guidelines do not constitute a set of general privacy protection principles; invasions of privacy by, for instance, candid photography, physical maltreatment, or defamation are outside their scope unless such acts are in one way or another associated with the handling of personal data. Thus, the Guidelines deal with the building-up and use of aggregates of data which are organised for retrieval, decision-making, research, surveys and similar purposes. It should be emphasized that the Guidelines are neutral with regard to the particular technology used; automatic methods are only one of the problems raised in the Guidelines although, particularly in the context of transborder data flows, this is clearly an important one.

[\(back to top of page\)](#)

B. DETAILED COMMENTS

General

39. The comments which follow relate to the actual Guidelines set out in the Annex to the Recommendation. They seek to clarify the debate in the Expert Group.

Paragraph 1: Definitions

40. The list of definitions has been kept short. The term "data controller" is of vital importance. It attempts to define a subject who, under domestic law, should carry ultimate responsibility for activities concerned with the processing of personal data. As defined, the data controller is a party who is legally competent to decide about the contents and use of data, regardless of whether or not such data are collected, stored, processed or disseminated by that party or by an agent on its behalf. The data controller may be a legal or natural person, public authority, agency or any other body. The definition excludes at least four categories which may be involved in the processing of data, viz:

- a) licensing authorities and similar bodies which exist in some Member countries and which authorise the processing of data but are not entitled to decide (in the proper sense of the word) what activities should be carried out and for what purposes;
- b) data processing service bureaux which carry out data processing on behalf of others;
- c) telecommunications authorities and similar bodies which act as mere conduits; and
- d) "dependent users" who may have access to data but who are not authorised to decide what data should be stored, who should be able to use them, etc. In implementing the Guidelines, countries may develop more complex schemes of levels and types of responsibilities.

Paragraphs 14 and 19 of the Guidelines provide a basis for efforts in this direction.

41. The terms "personal data" and "data subject" serve to underscore that the Guidelines are concerned with physical persons. The precise dividing line between personal data in the sense of information relating to identified or identifiable individuals and anonymous data may be difficult to draw and must be left to the regulation of each Member country. In principle, personal data convey information which by direct (e.g. a civil registration number) or indirect linkages (e.g. an address) may be connected to a particular physical person.

42. The term "transborder flows of personal data" restricts the application of certain provisions of the Guidelines to international data flows and consequently omits the data flow problems particular to federal states. The movements of data will often take place through electronic transmission but other means of data communication may also be involved. Transborder flows as understood in the Guidelines includes the transmission of data by satellite.

Paragraph 2: Area of application

43. The Section of the Memorandum dealing with the scope and purpose of the Guidelines introduces the issue of their

application to the automatic as against non-automatic processing of personal data. Paragraph 2 of the Guidelines, which deals with this problem, is based on two limiting criteria. The first is associated with the concept of personal data: the Guidelines apply to data which can be related to identified or identifiable individuals. Collections of data which do not offer such possibilities (collections of statistical data in anonymous form) are not included. The second criterion is more complex and relates to a specific risk element of a factual nature, viz. that data pose a danger to privacy and individual liberties. Such dangers can arise because of the use of automated data processing methods (the manner in which data are processed), but a broad variety of other possible risk sources is implied. Thus, data which are in themselves simple and factual may be used in a context where they become offensive to a data subject. On the other hand, the risks as expressed in Paragraph 2 of the Guidelines are intended to exclude data collections of an obviously innocent nature (e.g. personal notebooks). The dangers referred to in Paragraph 2 of the Guidelines should relate to privacy and individual liberties. However, the protected interests are broad (cf. paragraph 2 above) and may be viewed differently by different Member countries and at different times. A delimitation as far as the Guidelines are concerned and a common basic approach are provided by the principles set out in Paragraphs 7 to 13.

44. As explained in Paragraph 2 of the Guidelines, they are intended to cover both the private and the public sector. These notions may be defined differently by different Member countries.

Paragraph 3: Different degrees of sensitivity

45. The Guidelines should not be applied in a mechanistic way irrespective of the kind of data and processing activities involved. The framework provided by the basic principles in Part Two of the Guidelines permits Member countries to exercise their discretion with respect to the degree of stringency with which the Guidelines are to be implemented, and with respect to the scope of the measures to be taken. In particular, Paragraph 3(b) provides for many "trivial" cases of collection and use of personal data (cf. above) to be completely excluded from the application of the Guidelines. Obviously this does not mean that Paragraph 3 should be regarded as a vehicle for demolishing the standards set up by the Guidelines. But, generally speaking, the Guidelines do not presuppose their uniform implementation by Member countries with respect to details. For instance, different traditions and different attitudes by the general public have to be taken into account. Thus, in one country universal personal identifiers may be considered both harmless and useful whereas in another country they may be regarded as highly sensitive and their use restricted or even forbidden. In one country, protection may be afforded to data relating to groups and similar entities whereas such protection is completely non-existent in another country, and so forth. To conclude, some Member countries may find it appropriate to restrict the application of the Guidelines to the automatic processing of personal data. Paragraph 3(c) provides for such a limitation.

Paragraph 4: Exceptions to the Guidelines

46. To provide formally for exceptions in Guidelines which are part of a non-binding Recommendation may seem superfluous. However, the Expert Group has found it appropriate to include a provision dealing with this subject and stating that two general criteria ought to guide national policies in limiting the application of the Guidelines: exceptions should be as few as possible, and they should be made known to the public (e.g. through publication in an official government gazette). General knowledge of the existence of certain data or files would be sufficient to meet the second criterion, although details concerning particular data etc. may have to be kept secret. The formula provided in Paragraph 4 is intended to cover many different kinds of concerns and limiting factors, as it was obviously not possible to provide an exhaustive list of exceptions - hence the wording that they include national sovereignty, national security and public policy ("ordre public"). Another overriding national concern would be, for instance, the financial interests of the State ("crédit public"). Moreover, Paragraph 4 allows for different ways of implementing the Guidelines: it should be borne in mind that Member countries are at present at different stages of development with respect to privacy protection rules and institutions and will probably proceed at different paces, applying different strategies, e.g. the regulation of certain types of data or activities as compared to regulation of a general nature ("omnibus approach").

47. The Expert Group recognised that Member countries might apply the Guidelines differentially to different kinds of personal data. There may be differences in the permissible frequency of inspection, in ways of balancing competing interests such as the confidentiality of medical records versus the individual's right to inspect data relating to him, and so forth. Some examples of areas which may be treated differently are credit reporting, criminal investigation and banking. Member countries may also choose different solutions with respect to exceptions associated with, for example, research and statistics. An exhaustive enumeration of all such situations and concerns is neither required nor possible. Some of the subsequent paragraphs of the Guidelines and the comments referring to them provide further clarification of the area of application of the Guidelines and of the closely related issues of balancing opposing interests (compare with Paragraphs 7, 8, 17 and 18 of the Guidelines). To summarise, the Expert Group has assumed that exceptions will be limited to those which are necessary in a democratic society.

Paragraph 5: Federal countries

48. In Federal countries, the application of the Guidelines is subject to various constitutional limitations. Paragraph 5, accordingly, serves to underscore that no commitments exist to apply the Guidelines beyond the limits of constitutional competence.

Paragraph 6: Minimum standards

49. First, Paragraph 6 describes the Guidelines as minimum standards for adoption in domestic legislation. Secondly, and in consequence, it has been agreed that the Guidelines are capable of being supplemented by additional measures for the protection of privacy and individual liberties at the national as well as the international level.

Paragraph 7: Collection Limitation Principle

50. As an introductory comment on the principles set out in Paragraphs 7 to 14 of the Guidelines it should be pointed out

that these principles are interrelated and partly overlapping. Thus, the distinctions between different activities and stages involved in the processing of data which are assumed in the principles, are somewhat artificial and it is essential that the principles are treated together and studied as a whole. Paragraph 7 deals with two issues, viz.:

- a) limits to the collection of data which, because of the manner in which they are to be processed, their nature, the context in which they are to be used or other circumstances, are regarded as specially sensitive; and
- b) requirements concerning data collection methods. Different views are frequently put forward with respect to the first issue. It could be argued that it is both possible and desirable to enumerate types or categories of data which are per se sensitive and the collection of which should be restricted or even prohibited.

There are precedents in European legislation to this effect (race, religious beliefs, criminal records, for instance). On the other hand, it may be held that no data are intrinsically "private" or "sensitive" but may become so in view of their context and use. This view is reflected, for example, in the privacy legislation of the United States.

51. The Expert Group discussed a number of sensitivity criteria, such as the risk of discrimination, but has not found it possible to define any set of data which are universally regarded as sensitive. Consequently, Paragraph 7 merely contains a general statement that there should be limits to the collection of personal data. For one thing, this represents an affirmative recommendation to lawmakers to decide on limits which would put an end to the indiscriminate collection of personal data. The nature of the limits is not spelt out but it is understood that the limits may relate to:

data quality aspects (i.e. that it should be possible to derive information of sufficiently high quality from the data collected, that data should be collected in a proper information framework, etc.);

- limits associated with the purpose of the processing of data (i.e. that only certain categories of data ought to be collected and, possibly, that data collection should be restricted to the minimum necessary to fulfil the specified purpose);
- "earmarking" of specially sensitive data according to traditions and attitudes in each Member country;
- limits to data collection activities of certain data controllers;
- civil rights concerns.

52. The second part of Paragraph 7 (data collection methods) is directed against practices which involve, for instance, the use of hidden data registration devices such as tape recorders, or deceiving data subjects to make them supply information. The knowledge or consent of the data subject is as a rule essential, knowledge being the minimum requirement. On the other hand, consent cannot always be imposed, for practical reasons. In addition, Paragraph 7 contains a reminder ("where appropriate") that there are situations where for practical or policy reasons the data subject's knowledge or consent cannot be considered necessary. Criminal investigation activities and the routine up-dating of mailing lists may be mentioned as examples. Finally, Paragraph 7 does not exclude the possibility of a data subject being represented by another party, for instance in the case of minors, mentally disabled person, etc.

Paragraph 8: Data Quality Principle

53. Requirements that data be relevant can be viewed in different ways. In fact, some members of the Expert Group hesitated as to whether such requirements actually fitted into the framework of privacy protection. The conclusion of the Group was to the effect, however, that data should be related to the purpose for which they are to be used. For instance, data concerning opinions may easily be misleading if they are used for purposes to which they bear no relation, and the same is true of evaluative data. Paragraph 8 also deals with accuracy, completeness and up-to-dateness which are all important elements of the data quality concept. The requirements in this respect are linked to the purposes of data, i.e. they are not intended to be more far-reaching than is necessary for the purposes for which the data are used. Thus, historical data may often have to be collected or retained; cases in point are social research, involving so-called longitudinal studies of developments in society, historical research, and the activities of archives. The "purpose test" will often involve the problem of whether or not harm can be caused to data subjects because of lack of accuracy, completeness and up-dating.

Paragraph 9: Purpose Specification Principle

54. The Purpose Specification Principle is closely associated with the two surrounding principles, i.e. the Data Quality Principle and the Use Limitation Principle. Basically, Paragraph 9 implies that before, and in any case not later than at the time data collection it should be possible to identify the purposes for which these data are to be used, and that later changes of purposes should likewise be specified. Such specification of purposes can be made in a number of alternative or complementary ways, e.g. by public declarations, information to data subjects, legislation, administrative decrees, and licences provided by supervisory bodies. According to Paragraphs 9 and 10, new purposes should not be introduced arbitrarily; freedom to make changes should imply compatibility with the original purposes. Finally, when data no longer serve a purpose, and if it is practicable, it may be necessary to have them destroyed (erased) or given an anonymous form. The reason is that control over data may be lost when data are no longer of interest; this may lead to risks of theft, unauthorised copying or the like.

Paragraph 10: Use Limitation Principle

55. This paragraph deals with uses of different kinds, including disclosure, which involve deviations from specified purposes. For instance, data may be transmitted from one computer to another where they can be used for unauthorised purposes without being inspected and thus disclosed in the proper sense of the word. As a rule the initially or subsequently specified purposes should be decisive for the uses to which data can be put. Paragraph 10 foresees two general exceptions to this principle: the consent of the data subject (or his representative - see Paragraph 52 above) and

the authority of law (including, for example, licences granted by supervisory bodies). For instance, it may be provided that data which have been collected for purposes of administrative decision-making may be made available for research, statistics and social planning.

Paragraph 11: Security Safeguards Principle

56. Security and privacy issues are not identical. However, limitations on data use and disclosure should be reinforced by security safeguards. Such safeguards include physical measures (locked doors and identification cards, for instance), organisational measures (such as authority levels with regard to access to data) and, particularly in computer systems, informational measures (such as enciphering and threat monitoring of unusual activities and responses to them). It should be emphasized that the category of organisational measures includes obligations for data processing personnel to maintain confidentiality. Paragraph 11 has a broad coverage. The cases mentioned in the provision are to some extent overlapping (e.g. access/disclosure). "Loss" of data encompasses such cases as accidental erasure of data, destruction of data storage media (and thus destruction of data) and theft of data storage media. "Modified" should be construed to cover unauthorised input of data, and "use" to cover unauthorised copying.

Paragraph 12: Openness Principle

57. The Openness Principle may be viewed as a prerequisite for the Individual Participation Principle (Paragraph 13); for the latter principle to be effective, it must be possible in practice to acquire information about the collection, storage or use of personal data. Regular information from data controllers on a voluntary basis, publication in official registers of descriptions of activities concerned with the processing of personal data, and registration with public bodies are some, though not all, of the ways by which this may be brought about. The reference to means which are "readily available" implies that individuals should be able to obtain information without unreasonable effort as to time, advance knowledge, travelling, and so forth, and without unreasonable cost.

Paragraph 13: Individual Participation Principle

58. The right of individuals to access and challenge personal data is generally regarded as perhaps the most important privacy protection safeguard. This view is shared by the Expert Group which, although aware that the right to access and challenge cannot be absolute, has chosen to express it in clear and fairly specific language. With respect to the individual sub-paragraphs, the following explanations are called for.

59. The right to access should as a rule be simple to exercise. This may mean, among other things, that it should be part of the day-to-day activities of the data controller or his representative and should not involve any legal process or similar measures. In some cases it may be appropriate to provide for intermediate access to data; for example, in the medical area a medical practitioner can serve as a go-between. In some countries supervisory organs, such as data inspection authorities, may provide similar services. The requirement that data be communicated within reasonable time may be satisfied in different ways. For instance, a data controller who provides information to data subjects at regular intervals may be exempted from obligations to respond at once to individual requests. Normally, the time is to be counted from the receipt of a request. Its length may vary to some extent from one situation to another depending on circumstances such as the nature of the data processing activity. Communication of such data "in a reasonable manner" means, among other things, that problems of geographical distance should be given due attention. Moreover, if intervals are prescribed between the times when requests for access must be met, such intervals should be reasonable. The extent to which data subjects should be able to obtain copies of data relating to them is a matter of implementation which must be left to the decision of each Member country.

60. The right to reasons in Paragraph 13(c) is narrow in the sense that it is limited to situations where requests for information have been refused. A broadening of this right to include reasons for adverse decisions in general, based on the use of personal data, met with sympathy in the Expert Group. However, on final consideration a right of this kind was thought to be too broad for insertion in the privacy framework constituted by the Guidelines. This is not to say that a right to reasons for adverse decisions may not be appropriate, e.g. in order to inform and alert a subject to his rights so that he can exercise them effectively.

61. The right to challenge in 13(c) and (d) is broad in scope and includes first instance challenges to data controllers as well as subsequent challenges in courts, administrative bodies, professional organs or other institutions according to domestic rules of procedure (compare with Paragraph 19 of the Guidelines). The right to challenge does not imply that the data subject can decide what remedy or relief is available (rectification, annotation that data are in dispute, etc.): such matters will be decided by domestic law and legal procedures. Generally speaking, the criteria which decide the outcome of a challenge are those which are stated elsewhere in the Guidelines.

Paragraph 14: Accountability Principle

62. The data controller decides about data and data processing activities. It is for his benefit that the processing of data is carried out. Accordingly, it is essential that under domestic law accountability for complying with privacy protection rules and decisions should be placed on the data controller who should not be relieved of this obligation merely because the processing of data is carried out on his behalf by another party, such as a service bureau. On the other hand, nothing in the Guidelines prevents service bureaux personnel, "dependent users" (see paragraph 40) and others from also being held accountable. For instance, sanctions against breaches of confidentiality obligations may be directed against all parties entrusted with the handling of personal information (cf. paragraph 19 of the Guidelines). Accountability under Paragraph 14 refers to accountability supported by legal sanctions, as well as to accountability established by codes of conduct, for instance.

Paragraphs 15-18: Basic Principles of International Application

63. The principles of international application are closely interrelated. Generally speaking, Paragraph 15 concerns respect by Member countries for each other's interest in protecting personal data, and the privacy and individual liberties of their nationals and residents. Paragraph 16 deals with security issues in a broad sense and may be said to correspond, at the international level, to Paragraph 11 of the Guidelines. Paragraphs 17 and 18 deal with restrictions on free flows of personal data between Member countries; basically, as far as protection of privacy and individual liberties is concerned, such flows should be admitted as soon as requirements of the Guidelines for the protection of these interests have been substantially, i.e. effectively, fulfilled. The question of other possible bases of restricting transborder flows of personal data is not dealt with in the Guidelines.

64. For domestic processing Paragraph 15 has two implications. First, it is directed against liberal policies which are contrary to the spirit of the Guidelines and which facilitate attempts to circumvent or violate protective legislation of other Member countries. However, such circumvention or violation, although condemned by all Member countries, is not specifically mentioned in this Paragraph as a number of countries felt it to be unacceptable that one Member country should be required to directly or indirectly enforce, extraterritorially, the laws of other Member countries. -- It should be noted that the provision explicitly mentions the re-export of personal data. In this respect, Member countries should bear in mind the need to support each other's efforts to ensure that personal data are not deprived of protection as a result of their transfer to territories and facilities for the processing of data where control is slack or non-existent.

65. Secondly, Member countries are implicitly encouraged to consider the need to adapt rules and practices for the processing of data to the particular circumstances which may arise when foreign data and data on non-nationals are involved. By way of illustration, a situation may arise where data on foreign nationals are made available for purposes which serve the particular interests of their country of nationality (e.g. access to the addresses of nationals living abroad).

66. As far as the Guidelines are concerned, the encouragement of international flows of personal data is not an undisputed goal in itself. To the extent that such flows take place they should, however, according to Paragraph 16, be uninterrupted and secure, i.e. protected against unauthorised access, loss of data and similar events. Such protection should also be given to data in transit, i.e. data which pass through a Member country without being used or stored with a view to usage in that country. The general commitment under Paragraph 16 should, as far as computer networks are concerned, be viewed against the background of the International Telecommunications Convention of Malaga-Torremolinos (25th October, 1973). According to that convention, the members of the International Telecommunications Union, including the OECD Member countries, have agreed, inter alia, to ensure the establishment, under the best technical conditions, of the channels and installations necessary to carry on the rapid and uninterrupted exchange of international telecommunications. Moreover, the members of ITU have agreed to take all possible measures compatible with the telecommunications system used to ensure the secrecy of international correspondence. As regards exceptions, the right to suspend international telecommunications services has been reserved and so has the right to communicate international correspondence to the competent authorities in order to ensure the application of internal laws or the execution of international conventions to which members of the ITU are parties. These provisions apply as long as data move through telecommunications lines. In their context, the Guidelines constitute a complementary safeguard that international flows of personal data should be uninterrupted and secure.

67. Paragraph 17 reinforces Paragraph 16 as far as relationships between Member countries are concerned. It deals with interests which are opposed to free transborder flows of personal data but which may nevertheless constitute legitimate grounds for restricting such flows between Member countries. A typical example would be attempts to circumvent national legislation by processing data in a Member country which does not yet substantially observe the Guidelines. Paragraph 17 establishes a standard of equivalent protection, by which is meant protection which is substantially similar in effect to that of the exporting country, but which need not be identical in form or in all respects. As in Paragraph 15, the re-export of personal data is specifically mentioned - in this case with a view to preventing attempts to circumvent the domestic privacy legislation of Member countries. - The third category of grounds for legitimate restrictions mentioned in Paragraph 17, concerning personal data of a special nature, covers situations where important interests of Member countries could be affected. Generally speaking, however, paragraph 17 is subject to Paragraph 4 of the Guidelines which implies that restrictions on flows of personal data should be kept to a minimum.

68. Paragraph 18 attempts to ensure that privacy protection interests are balanced against interests of free transborder flows of personal data. It is directed in the first place against the creation of barriers to flows of personal data which are artificial from the point of view of protection of privacy and individual liberties and fulfil restrictive purposes of other kinds which are thus not openly announced. However, Paragraph 18 is not intended to limit the rights of Member countries to regulate transborder flows of personal data in areas relating to free trade, tariffs, employment, and related economic conditions for intentional data traffic. These are matters which were not addressed by the Expert Group, being outside its Mandate.

Paragraph 19: National Implementation

69. The detailed implementation of Parts Two and Three of the Guidelines is left in the first place to Member countries. It is bound to vary according to different legal systems and traditions, and Paragraph 19 therefore attempts merely to establish a general framework indicating in broad terms what kind of national machinery is envisaged for putting the Guidelines into effect. The opening sentence shows the different approaches which might be taken by countries, both generally and with respect to control mechanisms (e.g. specially set up supervisory bodies, existing control facilities such as courts, public authorities, etc.).

70. In Paragraph 19(a) countries are invited to adopt appropriate domestic legislation, the word "appropriate" foreshadowing the judgement by individual countries of the appropriateness or otherwise of legislative solutions.

Paragraph 19(b) concerning self-regulation is addressed primarily to common law countries where non-legislative implementation of the Guidelines would complement legislative action. Paragraph 19(c) should be given a broad interpretation; it includes such means as advice from data controllers and the provision of assistance, including legal aid. Paragraph 19(d) permits different approaches to the issue of control mechanisms: briefly, either the setting-up of special supervisory bodies, or reliance on already existing control facilities, whether in the form of courts, existing public authorities or otherwise. Paragraph 19(e) dealing with discrimination is directed against unfair practices but leaves open the possibility of "benign discrimination" to support disadvantaged groups, for instance. The provision is directed against unfair discrimination on such bases as nationality and domicile, sex, race, creed, or trade union affiliation.

Paragraph 20: Information Exchange and Compatible Procedures

71. Two major problems are dealt with here, viz. (a) the need to ensure that information can be obtained about rules, regulations, decisions, etc. which implement the Guidelines, and (b) the need to avoid transborder flows of personal data being hampered by an unnecessarily complex and disparate framework of procedures and compliance requirements. The first problem arises because of the complexity of privacy protection regulation and data policies in general. There are often several levels of regulation (in a broad sense) and many important rules cannot be laid down permanently in detailed statutory provisions; they have to be kept fairly open and left to the discretion of lower-level decision-making bodies.

72. The importance of the second problem is, generally speaking, proportional to the number of domestic laws which affect transborder flows of personal data. Even at the present stage, there are obvious needs for co-ordinating special provisions on transborder data flows in domestic laws, including special arrangements relating to compliance control and, where required, licences to operate data processing systems.

Paragraph 21: Machinery for Co-operation

73. The provision on national procedures assumes that the Guidelines will form a basis for continued co-operation. Data protection authorities and specialised bodies dealing with policy issues in information and data communications are obvious partners in such a co-operation. In particular, the second purpose of such measures, contained in Paragraph 21(ii), i.e. mutual aid in procedural matters and requests for information, is future-oriented: its practical significance is likely to grow as international data networks and the complications associated with them become more numerous.

Paragraph 22: Conflicts of Laws

74. The Expert Group has devoted considerable attention to issues of conflicts of laws, and in the first place to the questions as to which courts should have jurisdiction over specific issues (choice of jurisdiction) and which system of law should govern specific issues (choice of law). The discussion of different strategies and proposed principles has confirmed the view that at the present stage, with the advent of such rapid changes in technology, and given the non-binding nature of the Guidelines, no attempt should be made to put forward specific, detailed solutions. Difficulties are bound to arise with respect to both the choice of a theoretically sound regulatory model and the need for additional experience about the implications of solutions which in themselves are possible.

75. As regards the question of choice of law, one way of approaching these problems is to identify one or more connecting factors which, at best, indicate one applicable law. This is particularly difficult in the case of international computer networks where, because of dispersed location and rapid movement of data, and geographically dispersed data processing activities, several connecting factors could occur in a complex manner involving elements of legal novelty. Moreover, it is not evident what value should presently be attributed to rules which by mechanistic application establish the specific national law to be applied. For one thing, the appropriateness of such a solution seems to depend upon the existence of both similar legal concepts and rule structures, and binding commitments of nations to observe certain standards of personal data protection. In the absence of these conditions, an attempt could be made to formulate more flexible principles which involve a search for a "proper law" and are linked to the purpose of ensuring effective protection of privacy and individual liberties. Thus, in a situation where several laws may be applicable, it has been suggested that one solution could be to give preference to the domestic law offering the best protection of personal data. On the other hand, it may be argued that solutions of this kind leave too much uncertainty, not least from the point of view of the data controllers who may wish to know, where necessary in advance, by which national systems of rules an international data processing system will be governed.

76. In view of these difficulties, and considering that problems of conflicts of laws might best be handled within the total framework of personal and non-personal data, the Expert Group has decided to content itself with a statement which merely signals the issues and recommends that Member countries should work towards their solution.

Follow-up

77. The Expert Group called attention to the terms of Recommendation 4 on the Guidelines which suggests that Member countries agree as soon as possible on specific procedures of consultation and co-operation for the application of the Guidelines.

[\(back to top of page\)](#)

Related Documents

[OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data](#)

[The 30th Anniversary of the OECD Privacy Guidelines](#)

© OECD. All rights reserved

[Terms and Conditions](#)

[Privacy Policy](#)

[MyOECD](#)

[Site Map](#)

[Contact Us](#)

University of Pennsylvania
Law Review

FOUNDED 1852

Formerly
American Law Register

Read 10/31

VOL. 154

JANUARY 2006

No. 3

This article
comes highly
recommended

ARTICLES

A TAXONOMY OF PRIVACY

DANIEL J. SOLOVE[†]

Privacy is a concept in disarray. Nobody can articulate what it means. As one commentator has observed, privacy suffers from "an embarrassment of meanings." Privacy is far too vague a concept to guide adjudication and

[†] Associate Professor, George Washington University Law School; J.D. Yale. A project such as this—one that attempts a taxonomy of the sprawling and complex concept of privacy—cannot be created by one individual alone. I owe an enormous debt of gratitude to many people who provided helpful comments on the manuscript or parts thereof at various stages in its development: Anita Allen, Howard Erichson, Jim Freeman, Robert Gellman, Rachel Godsil, Stan Karas, Orin Kerr, Raymond Ku, Chip Lupu, Jon Michaels, Larry Mitchell, Robert Post, Neil Richards, Michael Risinger, Peter Sand, Heidi Schooner, Paul Schwartz, Lior Strahilevitz, Charles Sullivan, Michael Sullivan, Peter Swire, Robert Tuttle, Sarah Waldeck, Richard Weisberg, and James Whitman. Thanks to Michael Weisberg and Brian Leiter for directing me to useful resources on systematics. I would also like to thank my research assistants, Poornima Ravishankar, Jessica Kahn, and Tiffany Stedman for their excellent assistance. Additionally, I benefited from helpful comments when I presented this paper at a workshop at Washington University and at a conference sponsored by the International Association of Privacy Professionals. The George Washington University School of Law scholarship fund provided generous support for this Article.

took forever
to write!

lawmaking, as abstract incantations of the importance of "privacy" do not fare well when pitted against more concretely stated countervailing interests.

In 1960, the famous torts scholar William Prosser attempted to make sense of the landscape of privacy law by identifying four different interests. But Prosser focused only on tort law, and the law of information privacy is significantly more vast and complex, extending to Fourth Amendment law, the constitutional right to information privacy, evidentiary privileges, dozens of federal privacy statutes, and hundreds of state statutes. Moreover, Prosser wrote over 40 years ago, and new technologies have given rise to a panoply of new privacy harms.

A new taxonomy to understand privacy violations is thus sorely needed. This Article develops a taxonomy to identify privacy problems in a comprehensive and concrete manner. It endeavors to guide the law toward a more coherent understanding of privacy and to serve as a framework for the future development of the field of privacy law.

INTRODUCTION	479
THE TAXONOMY	483
A. Information Collection	491
1. Surveillance	491
2. Interrogation	499
B. Information Processing	504
1. Aggregation	505
2. Identification	510
3. Insecurity	515
4. Secondary Use	518
5. Exclusion	521
C. Information Dissemination	523
1. Breach of Confidentiality	524
2. Disclosure	527
3. Exposure	532
4. Increased Accessibility	536
5. Blackmail	539
6. Appropriation	542
7. Distortion	546
D. Invasion	548
1. Intrusion	549
2. Decisional Interference	553

CONCLUSION	558
------------------	-----

INTRODUCTION

In Jorge Luis Borges's illuminating parable, *Everything and Nothing*, a gifted playwright creates breathtaking works of literature, populated with an unforgettable legion of characters, one after the other imbued with a unique, unforgettable personality.¹ Despite his spectacular feats of imagination, the playwright lives a life of despair. He can dream up a multitude of characters—become them, think like them, understand the depths of their souls—yet he himself has no core, no way to understand himself, no way to define who he is. At the end of the parable, before he dies, the playwright communicates his despair to God:

"I who have been so many men in vain want to be one and myself." The voice of the Lord answered from a whirlwind: "Neither am I anyone; I have dreamt the world as you dreamt your work, my Shakespeare, and among the forms in my dream are you, who like myself are many and no one."²

Privacy seems to be about everything, and therefore it appears to be nothing. As one commentator observed:

It is apparent that the word "privacy" has proven to be a powerful rhetorical battle cry in a plethora of unrelated contexts. . . . Like the emotive word "freedom," "privacy" means so many different things to so many different people that it has lost any precise legal connotation that it might once have had.³

Lillian BeVier writes: "Privacy is a chameleon-like word, used denotatively to designate a wide range of wildly disparate interests—from confidentiality of personal information to reproductive autonomy—and connotatively to generate goodwill on behalf of whatever interest is being asserted in its name."⁴ Other commentators have lamented that privacy is "vague and evanescent,"⁵ "protean,"⁶ and suffering from "an embarrassment of meanings."⁷ "Perhaps the most striking thing about the right to privacy,"

Where does it
come from

¹ JORGE LUIS BORGES, *Everything and Nothing*, in LABYRINTHS 248 (Donald A. Yates & James E. Irby eds., J.E.I. trans., 1964).

² *Id.* at 249.

³ 1 J. THOMAS MCCARTHY, THE RIGHTS OF PUBLICITY AND PRIVACY § 5.59 (2d ed. 2005).

⁴ Lillian R. BeVier, *Information About Individuals in the Hands of Government: Some Reflections on Mechanisms for Privacy Protection*, 4 WM. & MARY BILL RTS. J. 455, 458 (1995) (footnote omitted).

⁵ ARTHUR R. MILLER, THE ASSAULT ON PRIVACY: COMPUTERS, DATA BANKS, AND DOSSIERS 25 (1971) (citation omitted).

⁶ Tom Gerety, *Redefining Privacy*, 12 HARV. C.R.-C.L. L. REV. 233, 234 (1977).

⁷ KIM LANE SCHEPPELE, LEGAL SECRETS 184-85 (1988).

philosopher Judith Jarvis Thomson has observed, "is that nobody seems to have any very clear idea what it is."⁸

Often, privacy problems are merely stated in knee-jerk form: "That violates my privacy!" When we contemplate an invasion of privacy—such as having our personal information gathered by companies in databases—we instinctively recoil. Many discussions of privacy appeal to people's fears and anxieties.⁹ What commentators often fail to do, however, is translate those instincts into a reasoned, well-articulated account of why privacy problems are harmful. When people claim that privacy should be protected, it is unclear precisely what they mean. This lack of clarity creates a difficulty when making policy or resolving a case because lawmakers and judges cannot easily articulate the privacy harm. The interests on the other side—free speech, efficient consumer transactions, and security—are often much more readily articulated. Courts and policymakers frequently struggle in recognizing privacy interests, and when this occurs, cases are dismissed or laws are not passed. The result is that privacy is not balanced against countervailing interests.

or just public
pointer to us?

Abstract incantations of "privacy" are not nuanced enough to capture the problems involved. The *9/11 Commission Report*, for example, recommends that, as government agencies engage in greater information sharing with each other and with businesses, they should "safeguard the privacy of individuals about whom information is shared."¹⁰ But what does safeguarding "privacy" mean? Without an understanding of what the privacy problems are, how can privacy be addressed in a meaningful way?

Many commentators have spoken of privacy as a unitary concept with a uniform value, which is unvarying across different situations. In contrast, I have argued that privacy violations involve a variety of types of harmful or problematic activities.¹¹ Consider the following examples of activities typically referred to as privacy violations:

⁸ Judith Jarvis Thomson, *The Right to Privacy*, in *PHILOSOPHICAL DIMENSIONS OF PRIVACY: AN ANTHOLOGY* 272, 272 (Ferdinand David Schoeman ed., 1984).

⁹ See James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 *YALE L.J.* 1151, 1154 (2004) ("[T]he typical privacy article rests its case precisely on an appeal to its reader's intuitions and anxieties about the evils of privacy violations.").

¹⁰ NAT'L COMM'N ON TERRORIST ATTACKS UPON THE U.S., *THE 9/11 COMMISSION REPORT* 394 (2004).

¹¹ Daniel J. Solove, *Conceptualizing Privacy*, 90 *CAL. L. REV.* 1087, 1130 (2002) [hereinafter Solove, *Conceptualizing Privacy*]. In contrast to attempts to conceptualize privacy by isolating one or more common "essential" or "core" characteristics, I concluded that there is no singular essence found in all "privacy" violations. See *id.* at 1095-99 (concluding that "the quest for a common denominator or essence . . . can sometimes lead to confusion").

- A newspaper reports the name of a rape victim.¹²
- Reporters deceitfully gain entry to a person's home and secretly photograph and record the person.¹³
- New X-ray devices can see through people's clothing, amounting to what some call a "virtual strip-search."¹⁴
- The government uses a thermal sensor device to detect heat patterns in a person's home.¹⁵
- A company markets a list of five million elderly incontinent women.¹⁶
- Despite promising not to sell its members' personal information to others, a company does so anyway.¹⁷

These violations are clearly not the same. Despite the wide-ranging body of law addressing privacy issues today, commentators often lament the law's inability to adequately protect privacy.¹⁸ Courts and policymakers frequently have a singular view of privacy in mind when they assess whether or not an activity violates privacy. As a result, they either conflate distinct privacy problems despite significant differences or fail to recognize a problem entirely. Privacy problems are frequently misconstrued or inconsistently recognized in the law. The concept of "privacy" is far too vague to guide adjudication and lawmaking. How can privacy be addressed in a manner that is non-reductive and contextual, yet simultaneously useful in deciding cases and making sense of the multitude of privacy problems we face?

In this Article, I provide a framework for how the legal system can come to a better understanding of privacy. I aim to develop a taxonomy that focuses more specifically on the different kinds of activities that impinge upon privacy. I endeavor to shift focus away from the vague term "privacy"

¹² See *Florida Star v. B.J.F.*, 491 U.S. 524, 527 (1989).

¹³ See *Dietemann v. Time, Inc.*, 449 F.2d 245, 246 (9th Cir. 1971).

¹⁴ See *Beyond X-ray Vision: Can Big Brother See Right Through Your Clothes?*, DISCOVER, July 2002, at 24; Guy Gugliotta, *Tech Companies See Market for Detection: Security Techniques Offer New Precision*, WASH. POST, Sept. 28, 2001, at A8.

¹⁵ See *Kyllo v. United States*, 533 U.S. 27, 29 (2001).

¹⁶ See Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,461, 82,467 (Dec. 28, 2000) (codified at 45 C.F.R. pts. 160 & 164).

¹⁷ See *In re GeoCities*, 127 F.T.C. 94, 97-98 (1999).

¹⁸ See, e.g., Joel R. Reidenberg, *Privacy in the Information Economy: A Fortress or Frontier for Individual Rights?*, 44 FED. COMM. L.J. 195, 208 (1992) ("The American legal system does not contain a comprehensive set of privacy rights or principles that collectively address the acquisition, storage, transmission, use and disclosure of personal information within the business community."); Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1611 (1999) ("At present, however, no successful standards, legal or otherwise, exist for limiting the collection and utilization of personal data in cyberspace.").

and toward the specific activities that pose privacy problems. Although various attempts at explicating the meaning of "privacy" have been made, few have attempted to identify privacy problems in a comprehensive and concrete manner.¹⁹ The most famous attempt was undertaken in 1960 by the legendary torts scholar William Prosser. He discerned four types of harmful activities redressed under the rubric of privacy:

1. Intrusion upon the plaintiff's seclusion or solitude, or into his private affairs.
2. Public disclosure of embarrassing private facts about the plaintiff.
3. Publicity which places the plaintiff in a false light in the public eye.
4. Appropriation, for the defendant's advantage, of the plaintiff's name or likeness.²⁰

Prosser's great contribution was to synthesize the cases that emerged from Samuel Warren and Louis Brandeis's famous law review article, *The Right to Privacy*.²¹

However, Prosser focused only on tort law. American privacy law is significantly more vast and complex, extending beyond torts to the constitutional "right to privacy," Fourth Amendment law, evidentiary privileges, dozens of federal privacy statutes, and hundreds of state privacy statutes.²²

¹⁹ In 1967, Alan Westin identified four "basic states of individual privacy": (1) solitude; (2) intimacy; (3) anonymity; and (4) reserve ("the creation of a psychological barrier against unwanted intrusion"). ALAN F. WESTIN, *PRIVACY AND FREEDOM* 31-32 (1967). These categories focus mostly on spatial distance and separateness; they fail to capture the many different dimensions of informational privacy. In 1992, Ken Gormley surveyed the law of privacy. See generally Ken Gormley, *One Hundred Years of Privacy*, 1992 WIS. L. REV. 1335. His categories—tort privacy, Fourth Amendment privacy, First Amendment privacy, fundamental-decision privacy, and state constitutional privacy—are based on different areas of law rather than on a more systemic conceptual account of privacy. *Id.* at 1340. In 1998, Jerry Kang defined privacy as a union of three overlapping clusters of ideas: (1) physical space ("the extent to which an individual's territorial solitude is shielded from invasion by unwanted objects or signals"); (2) choice ("an individual's ability to make certain significant decisions without interference"); and (3) flow of personal information ("an individual's control over the processing—i.e., the acquisition, disclosure, and use—of personal information"). Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1202-03 (1998). Kang's understanding of privacy is quite rich, but the breadth of the categories limits their usefulness in law. The same is true of the three categories identified by philosopher Judith DeCew: (1) "informational privacy"; (2) "accessibility privacy"; and (3) "expressive privacy." JUDITH W. DECEW, *IN PURSUIT OF PRIVACY: LAW, ETHICS, AND THE RISE OF TECHNOLOGY* 75-77 (1997).

²⁰ William L. Prosser, *Privacy*, 48 CAL. L. REV. 383, 389 (1960).

²¹ Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195-96 (1890).

²² See Anita L. Allen, *Privacy in American Law*, in *PRIVACIES: PHILOSOPHICAL EVALUATIONS* 19, 26 (Beate Rössler ed., 2004) ("American privacy law is impressive in its

The Freedom of Information Act contains two exemptions to protect against an "unwarranted invasion of personal privacy."²³ Numerous state public records laws also contain privacy exemptions.²⁴ Many state constitutions contain provisions explicitly providing for a right to privacy.²⁵

Moreover, Prosser wrote over forty years ago, before the breathtaking rise of the Information Age. New technologies have given rise to a panoply of different privacy problems, and many of them do not readily fit into Prosser's four categories. Therefore, a new taxonomy to address privacy violations for contemporary times is sorely needed.

The taxonomy I develop is an attempt to identify and understand the different kinds of socially recognized privacy violations, one that hopefully will enable courts and policymakers to better balance privacy against countervailing interests. The purpose of this taxonomy is to aid in the development of the law that addresses privacy. Although the primary focus will be on the law, this taxonomy is not simply an attempt to catalog existing laws, as was Prosser's purpose. Rather, it is an attempt to understand various privacy harms and problems that have achieved a significant degree of social recognition. ~~I will frequently use the law as a source for determining what privacy violations society recognizes.~~ However, my aim is not simply to take stock of where the law currently stands today, but to provide a useful framework for its future development.

THE TAXONOMY

Privacy cannot be understood independently from society. As sociologist Barrington Moore aptly observes, "the need for privacy is a socially

quantity and scope."). For a survey of the vast scope of the law of information privacy, see DANIEL J. SOLOVE & MARC ROTENBERG, *INFORMATION PRIVACY LAW* (2003).

²³ 5 U.S.C. § 552(b)(6) (2000) (exempting "personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy"); *id.* § 552b(c)(7) (exempting disclosure of "investigatory records compiled for law enforcement purposes that "constitute an unwarranted invasion of personal privacy" at open meetings).

²⁴ See Daniel J. Solove, *Access and Aggregation: Public Records, Privacy and the Constitution*, 86 MINN. L. REV. 1137, 1160-64 (2002) (examining federal and state freedom of information acts and their exemptions).

²⁵ See, e.g., ALASKA CONST. art. I, § 22 ("The right of the people to privacy is recognized and shall not be infringed."); CAL. CONST. art. I, § 1 ("All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy."); FLA. CONST. art. I, § 23 ("Every natural person has the right to be let alone and free from governmental intrusion into the person's private life except as otherwise provided herein.").

Philosophy

created need. Without society there would be no need for privacy."²⁶ Society is fraught with conflict and friction. Individuals, institutions, and governments can all engage in activities that have problematic effects on the lives of others.

Privacy is the relief from a range of kinds of social friction. It enables people to engage in worthwhile activities in ways that they would otherwise find difficult or impossible. Of course, privacy is not freedom from all forms of social friction; rather, it is protection from a cluster of related activities that impinge upon people in related ways. This taxonomy attempts to identify and organize these problematic activities.²⁷ These activities often are not inherently problematic or harmful. If a person consents to most of these activities, there is no privacy violation.²⁸ Thus, if a couple invites another to watch them have sex, this observation would not constitute a privacy violation. Without consent, however, it most often would.

Of course, declaring that an activity is harmful or problematic does not automatically imply that there should be legal redress, since there may be valid reasons why the law should not get involved or why countervailing interests should prevail. As Anita Allen argues, there are certainly times when people should be held accountable for their private activities.²⁹ The

²⁶ BARRINGTON MOORE, JR., *PRIVACY: STUDIES IN SOCIAL AND CULTURAL HISTORY* 73 (1984).

²⁷ This taxonomy focuses on activities of others that can and do create privacy harms or problems. The full equation for a privacy violation or problem is the existence of a certain activity that causes harms or problems affecting a private matter or activity. This taxonomy focuses on the first part of the equation (harmful or problematic activities) rather than on what constitutes a private matter or activity. Since the question of which matters and activities are private is too culturally variable and contextual, this taxonomy focuses on potentially harmful or problematic activities, about which I believe meaningful generalizations can be made. Despite the fact that the taxonomy limits its focus to the activities that harm or cause problems for private matters or activities, I believe that the taxonomy serves as a useful way for the law to approach and comprehend privacy problems. While the entire "privacy equation" must be worked out in each particular case, the taxonomy aims to carve up the landscape in a way that the law can begin to comprehend and engage. All taxonomies are generalizations based upon a particular focus, and they are valuable only insofar as they are useful. It is my hope that this taxonomy succeeds by this metric.

²⁸ Of course, there remains the issue of what constitutes valid consent, as there are many occasions in which people affirmatively give out information that should not be assumed to be consensual. See Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1397-98 (2000) (arguing that "people are demonstrably bad at" assessing the risk of future harms that may flow from the piecemeal, otherwise consensual collection of their private data); Schwartz, *supra* note 18, at 1661-64 (1999) (discussing the legal fiction of consent in the context of the Internet, specifically the use of boilerplate consent forms that do not require user agreement before taking effect).

²⁹ See ANITA L. ALLEN, *WHY PRIVACY ISN'T EVERYTHING* 2, 146 (2003) (discussing tort theories available as recourse for the invasion of privacy in the context of sexual harassment claims).

purpose of this taxonomy is not to argue that the law should or should not protect against certain activities that affect privacy. Rather, the goal is simply to define the activities and explain why and how they can cause trouble. The question of when and how the law should regulate can only be answered in each specific context in which the question arises. But attempts to answer this question are increasingly suffering because of confusion about defining the troublesome activities that fall under the rubric of privacy. This taxonomy will aid us in analyzing various privacy problems so the law can better address them and balance them with opposing interests.

In devising a taxonomy, there are many different ways to go about carving up the landscape. I focus on the activities that invade privacy. The purpose of the taxonomy is to assist the legal system in grappling with the concept of privacy. Since the goal of the law is to have privacy protections that best prevent and redress particular problems, we need to first understand the problems in order to evaluate the effectiveness of the protections.

Therefore, my focus is on activities that create problems. I aim to show that these activities differ significantly yet share many commonalities. Privacy is too complicated a concept to be boiled down to a single essence. Attempts to find such an essence often end up being too broad and vague, with little usefulness in addressing concrete issues. Elsewhere, I have argued that privacy is best understood as a family resemblance concept.³⁰ As philosopher Ludwig Wittgenstein explained, certain things may not share one common characteristic, but they nevertheless are "related to one another in many different ways."³¹ Wittgenstein analogized to members of a family, who generally share some traits with each other (eye color, height, facial structure, hair color, etc.), although they may not have one common trait.³² There is, however, "a complicated network of similarities overlapping and criss-crossing."³³

The term "privacy" is an umbrella term, referring to a wide and disparate group of related things. The use of such a broad term is helpful in some contexts yet quite unhelpful in others. Consider, for example, the term "animal." "Animal" refers to a large group of organisms—there are mammals, birds, reptiles, fish, and so on. Within each of these groups are subgroups. For some purposes, using the term "animal" will suffice. Suppose Sue asks Bob, "How many animals are in the zoo?" Bob does not need to know anything more specific in order to answer this question. The use of

³⁰ Solove, *Conceptualizing Privacy*, *supra* note 11, at 1096-99.

³¹ LUDWIG WITTGENSTEIN, *PHILOSOPHICAL INVESTIGATIONS* § 65 (G.E.M. Anscombe trans., 1968) (1958).

³² *Id.* § 67.

³³ *Id.* § 66.

the term "animal" in this sentence will be perfectly clear in most contexts. Now suppose Sue wants Bob to bring her a dog. She will not get very far by saying, "Bring me an animal." Rather, she will specify the kind of animal she wants. Even saying "dog" probably will not be adequate, since Sue probably wants a specific kind of dog. As with the term "animal," there are many times when using the general term "privacy" will work well. But there are times where more specificity is required. Using the general term "privacy" can result in the conflation of different kinds of problems and can lead to understandings of the meaning of "privacy" that distract courts and policymakers from addressing the issues before them.

The taxonomy demonstrates that there are connections between different harms and problems. It is no accident that various problems are referred to as privacy violations; they bear substantial similarities to each other. But we also must recognize where they diverge. The goal is to define more precisely what the problem is in each context—how it is unique, how it differs from other problems, and how it is related to other types of privacy problems.

Often these problems involve harms to individuals. Certain kinds of harm, such as physical injuries, are very easy to articulate and understand. A privacy violation presents a more difficult case. Warren and Brandeis spoke of privacy as an incorporeal rather than a physical injury. They noted that the law was beginning to recognize nonphysical harms and that "modern enterprise and invention have, through invasions upon [a person's] privacy, subjected him to mental pain and distress, far greater than could be inflicted by mere bodily injury."³⁴ Privacy, contended the authors, involves "injury to the feelings."³⁵

The harms Warren and Brandeis spoke of are dignitary harms. The classic example of such a harm is reputational injury. As Warren and Brandeis noted, defamation law has long recognized and redressed this kind of injury that lowered people in the esteem of others.³⁶ But as Warren and Brandeis understood, and as this taxonomy will demonstrate, there are other kinds of dignitary harm beyond reputational injury. These are the harms of incivility, lack of respect, or causing emotional angst. At the time Warren and Brandeis wrote, they were concerned that such dignitary harms might strike some as too ethereal to be legally cognizable.³⁷ Their project aimed to demonstrate that these were genuine harms that were legally cogniza-

What is
the harm?

³⁴ Warren & Brandeis, *supra* note 21, at 196.

³⁵ *Id.* at 197.

³⁶ *Id.*

³⁷ See *id.* at 198 (noting that traditionally, "our system . . . does not afford a remedy even for mental suffering which results from mere contumely and insult").

ble.³⁸ And they succeeded, as Prosser emphatically demonstrated in 1960 by collecting hundreds of cases.³⁹

There is another, more modern kind of privacy problem that does not readily fit with this dignitary understanding of harm. These problems are more structural in nature. I refer to them as “architectural” problems.⁴⁰ They involve less the overt insult or reputational harm to a person and more the creation of the risk that a person might be harmed in the future. They are akin, in many ways, to environmental harms or pollution. In the taxonomy, two kinds of architectural issues emerge most often. First is the enhancement of the risk that a harm will occur. Activities involving a person’s information, for example, might create a greater risk of that person being victimized by identity theft or fraud. Such risk-enhancing activities increase the chances of the individual suffering dignitary harms as well as monetary or physical harms. Second, a particular activity can upset the balance of social or institutional power in undesirable ways. A particular individual may not be harmed directly, but this balance of power can affect that person’s life. The classic example is law enforcement officials having too much power, which can alter the way people engage in their activities. People’s behavior might be chilled, making them less likely to attend political rallies or criticize popular views. Surveillance can also have these effects. This kind of harm is often referred to as a “chilling effect.”⁴¹ Imbalances in power can also be risk enhancing, in that they increase the risk of abuses of power.

SSN leak

When we speak of these activities, we often focus on how they affect an individual’s life. This does not mean that privacy is an individualistic right. Philosopher John Dewey astutely argued that individual rights need not be justified as the immutable possessions of individuals; instead, they are instrumental in light of “the contribution they make to the welfare of the community.”⁴² Employing a similar insight, several scholars contend that privacy is “constitutive” of society. Constitutive privacy understands pri-

³⁸ See *id.* at 197 (positing that a “legal remedy for [a privacy] injury” would treat the “wound[ing of] feelings[] as a substantive cause of action”).

³⁹ See Prosser, *supra* note 20, at 389 (examining over three hundred cases to find legal recognition of “four distinct kinds of invasion of four different interests of the plaintiff”).

⁴⁰ See DANIEL J. SOLOVE, *THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE* 97-101 (2004) [hereinafter SOLOVE, *THE DIGITAL PERSON*] (identifying the influence of “an architecture that structures power, a regulatory framework that governs how information is disseminated, collected and networked” on protecting privacy).

⁴¹ See, e.g., *Laird v. Tatum*, 408 U.S. 1, 13 (1972) (confronting the alleged “chilling effect” that Army surveillance had on “lawful and peaceful civilian political activity”).

⁴² JOHN DEWEY, *Liberalism and Civil Liberties*, in 11 *LATER WORKS* 372, 373 (Jo Ann Boydston ed., S. Ill. Univ. Press 1987) (1936).

vacy harms as extending beyond the "mental pain and distress" caused to particular individuals; privacy harms affect the nature of society and impede individual activities that contribute to the greater social good. Spiros Simitis recognizes that "privacy considerations no longer arise out of particular individual problems; rather, they express conflicts affecting everyone."⁴³ Robert Post contends that the tort of invasion of privacy "safeguards rules of civility that in some significant measure constitute both individuals and community."⁴⁴ The theory of constitutive privacy has been further developed by Julie Cohen and Paul Schwartz, who both argue that privacy is a constitutive element of a civil society.⁴⁵

In the taxonomy that follows, there are four basic groups of harmful activities: (1) information collection, (2) information processing, (3) information dissemination, and (4) invasion. Each of these groups consists of different related subgroups of harmful activities.

I have arranged these groups around a model that begins with the data subject—the individual whose life is most directly affected by the activities classified in the taxonomy. From that individual, various entities (other people, businesses, and the government) collect information. The collection of this information itself can constitute a harmful activity. Not all information collection is harmful, but certain kinds of collection can be. Those that collect the data (the "data holders") then process it—they store it, combine it, manipulate it, search it, and use it. I label these activities as "information processing."⁴⁶ The next step is "information dissemination," in which the data holders transfer the information to others or release the information. The general progression from information collection to processing to dissemination is the data moving further away from the control of the individual. The last grouping of activities is "invasions," which involve impinge-

⁴³ Spiros Simitis, *Reviewing Privacy in an Information Society*, 135 U. PA. L. REV. 707, 709 (1987). In analyzing the problems of federal legislative policymaking on privacy, Priscilla Regan demonstrates the need for understanding privacy in terms of its social benefits. See PRISCILLA M. REGAN, *LEGISLATING PRIVACY*, xiv (1995) ("[A]nalysis of congressional policy making reveals that little attention was given to the possibility of a broader social importance of privacy.").

⁴⁴ Robert C. Post, *The Social Foundations of Privacy: Community and Self in the Common Law Tort*, 77 CAL. L. REV. 957, 959 (1989).

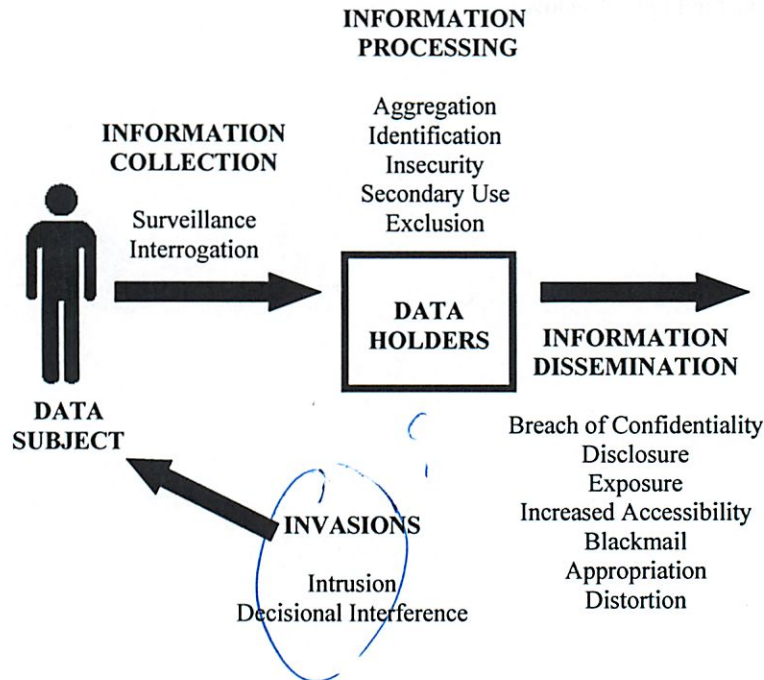
⁴⁵ See Cohen, *supra* note 28, at 1427-28 ("Informational privacy, in short, is a constitutive element of a civil society in the broadest sense of the term."); Schwartz, *supra* note 18, at 1613 ("[I]nformation privacy is best conceived of as a constitutive element of civil society."); see also Ruth Gavison, *Privacy and the Limits of Law*, 89 YALE L.J. 421, 455 (1980) ("Privacy is also essential to democratic government because it fosters and encourages the moral autonomy of the citizen, a central requirement of a democracy.").

⁴⁶ I borrow the term "processing" from the European Union Data Protection Directive. See Council Directive 95/46, art. 2(b), 1995 O.J. (L 281) 31 (EC).

ments directly on the individual. Instead of the progression away from the individual, invasions progress toward the individual and do not necessarily involve information. The relationship between these different groupings is depicted in Figure 1 below.⁴⁷

⁴⁷ I thank Peter Swire for suggesting and helping to develop this diagram.

Figure 1



The first group of activities that affect privacy involves information collection. *Surveillance* is the watching, listening to, or recording of an individual's activities. *Interrogation* consists of various forms of questioning or probing for information.

A second group of activities involves the way information is stored, manipulated, and used—what I refer to collectively as “information processing.” *Aggregation* involves the combination of various pieces of data about a person. *Identification* is linking information to particular individuals. *Insecurity* involves carelessness in protecting stored information from leaks and improper access. *Secondary use* is the use of information collected for one purpose for a different purpose without the data subject's consent. *Exclusion* concerns the failure to allow the data subject to know about the data that others have about her and participate in its handling and use. These activities do not involve the gathering of data, since it has already been collected. Instead, these activities involve the way data is maintained and used.

The third group of activities involves the dissemination of information. *Breach of confidentiality* is breaking a promise to keep a person's information confidential. *Disclosure* involves the revelation of truthful information about a person that impacts the way others judge her character. *Exposure* involves revealing another's nudity, grief, or bodily functions. *Increased accessibility* is amplifying the accessibility of information. *Blackmail* is the threat to disclose personal information. *Appropriation* involves the use of the data subject's identity to serve the aims and interests of another. *Distortion* consists of the dissemination of false or misleading information about individuals. Information dissemination activities all involve the spreading or transfer of personal data or the threat to do so.

The fourth and final group of activities involves invasions into people's private affairs. Invasion, unlike the other groupings, need not involve personal information (although in numerous instances, it does). *Intrusion* concerns invasive acts that disturb one's tranquility or solitude. *Decisional interference* involves the government's incursion into the data subject's decisions regarding her private affairs.

A. *Information Collection*

Information collection creates disruption based on the process of data gathering. Even if no information is revealed publicly, information collection can create harm. I will identify two forms of information collection: (1) surveillance and (2) interrogation.

1. Surveillance

For a long time, surveillance has been viewed as problematic. The term "Peeping Tom" originates from a legend dating back to 1050. When Lady Godiva rode naked on a horse in the city of Coventry to protest taxes, a young man named Tom gawked at her, and he was punished by being blinded.⁴⁸ Today, many states have Peeping Tom laws. South Carolina, for example, criminalizes "peep[ing] through windows, doors, or other like places, on or about the premises of another, for the purpose of spying upon or invading the privacy of the persons spied upon and any other conduct of a

⁴⁸ CLAY CALVERT, VOYEUR NATION 36-38 (2000); Avishai Margalit, *Privacy in the Decent Society*, 68 SOC. RES. 255, 259 (2001). In another version of the story, Tom is not blinded by others, but inexplicably struck blind upon looking at her after Lady Godiva asked the townspeople not to look. BBC, *Beyond the Broadcast, Making History: Lady Godiva of Coventry*, http://www.bbc.co.uk/education/beyond/factsheets/makhist/makhist6_prog9d.shtml (last visited Jan. 21, 2006).

similar nature, that tends to invade the privacy of others."⁴⁹ Some states prohibit two-way mirrors in certain areas.⁵⁰

As with visual surveillance, audio surveillance has long been viewed as troubling. William Blackstone noted that eavesdropping was a common law crime, and defined it as "listen[ing] under walls or windows, or the eaves of a house, to hearken after discourse, and thereupon to frame slanderous and mischievous tales."⁵¹ These attitudes persisted after the emergence of electronic eavesdropping. As early as 1862, California prohibited the interception of telegraph communications.⁵² Soon after telephone wiretapping began in the 1890s, several states prohibited it, such as California in 1905.⁵³ By 1928, over half the states had made wiretapping a crime.⁵⁴ Justice Holmes referred to wiretapping as a "dirty business,"⁵⁵ and Justice Frankfurter called it "odious."⁵⁶ When the Supreme Court held in the 1928 case *Olmstead v. United States* that the Fourth Amendment did not protect against wiretapping,⁵⁷ Congress responded six years later by making wiretapping a federal crime.⁵⁸ In 1967, the Supreme Court changed its position on wiretapping, overruling *Olmstead* in *Katz v. United States*.⁵⁹ One year later, Congress passed the Omnibus Crime Control and Safe Streets Act of 1968, Title III of which provided comprehensive protection against wiretapping.⁶⁰ Title III required law enforcement officials to obtain a warrant before

⁴⁹ S.C. CODE ANN. § 16-17-470(A) (2003); see also GA. CODE ANN. § 16-11-61 (2003) (criminalizing being a "peeping Tom" when "on or about the premises of another"); LA. REV. STAT. ANN. § 14:284 (2004) (defining "Peeping Tom" and setting forth the penalty); N.C. GEN. STAT. § 14-202 (Supp. 2004) (criminalizing peeping as a Class 1 misdemeanor); VA. CODE ANN. § 18.2-130 (2004) (criminalizing peeping or spying into a "dwelling or enclosure").

⁵⁰ For example, in California, "[a]ny person who installs or who maintains . . . any two-way mirror permitting observation of any restroom, toilet, bathroom, washroom, shower, locker room, fitting room, motel room, or hotel room is guilty of a misdemeanor." CAL. PENAL CODE § 653n (West 1988).

⁵¹ 4 WILLIAM BLACKSTONE, COMMENTARIES *169.

⁵² SAMUEL DASH ET AL., THE EAVESDROPPERS 25-26 (1959).

⁵³ *Id.* at 8, 25.

⁵⁴ Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 841 (2004) (citing *Berger v. New York*, 388 U.S. 41, 45 (1967)).

⁵⁵ *Olmstead v. United States*, 277 U.S. 438, 470 (1928) (Holmes, J., dissenting).

⁵⁶ *On Lee v. United States*, 343 U.S. 747, 758-59 (1952) (Frankfurter, J., dissenting).

⁵⁷ 277 U.S. at 466.

⁵⁸ See Federal Communications Act of 1934, Pub. L. No. 90-351, § 2520, 48 Stat. 1103 (codified as amended at 47 U.S.C. § 605 (2000)).

⁵⁹ 389 U.S. 347, 353 (1967).

⁶⁰ Pub. L. No. 90-351, ch. 119, 82 Stat. 212 (codified as amended at 18 U.S.C. §§ 2510-2522 (2000)).

wiretapping and criminalized wiretaps by private parties.⁶¹ Congress amended Title III in 1986 with the Electronic Communications Privacy Act (ECPA), expanding Title III's protections from wiretapping to additional forms of electronic surveillance.⁶²

What is the harm if people or the government watch or listen to us? Certainly, we all watch or listen, even when others may not want us to, and we often do not view this as problematic. However, when done in a certain manner—such as continuous monitoring—surveillance has problematic effects. For example, people expect to be looked at when they ride the bus or subway, but persistent gawking can create feelings of anxiety and discomfort.

amt of looking

Not only can direct awareness of surveillance make a person feel extremely uncomfortable, but it can also cause that person to alter her behavior. Surveillance can lead to self-censorship and inhibition.⁶³ Because of its inhibitory effects, surveillance is a tool of social control, enhancing the power of social norms, which work more effectively when people are being observed by others in the community.⁶⁴ John Gilliom observes: "Surveillance of human behavior is in place to control human behavior, whether by limiting access to programs or institutions, monitoring and affecting behavior within those arenas, or otherwise enforcing rules and norms by observing and recording acts of compliance and deviance."⁶⁵ This aspect of surveillance does not automatically make it harmful, though, since social control can be beneficial and every society must exercise a sizeable degree of social control. For example, surveillance can serve as a deterrent to crime. Many people desire the discipline and control surveillance can bring. Jeff Rosen observes that Britain's closed circuit television (CCTV)—a net-

⁶¹ 82 Stat. 213-14 (codified as amended at 18 U.S.C. § 2511 (2000)).

⁶² See Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended at 18 U.S.C. §§ 2510-2520, 2701-2711, 3121-3127 (2000)) (expanding Titles I-III to protect "wire, oral, or electronic communications").

⁶³ See Kang, *supra* note 19, at 1193, 1260 ("Simply put, surveillance leads to self-censorship."); Peter P. Swire, *Financial Privacy and the Theory of High-Tech Government Surveillance*, 77 WASH. U. L.Q. 461, 473 (1999) ("If I know I am under surveillance, I might . . . restrict my activities, so that nothing embarrassing or otherwise harmful could be detected.").

⁶⁴ As Judge Posner notes, "norms are more effective when people are under the observation of their peers." RICHARD A. POSNER, *THE PROBLEMATICS OF MORAL AND LEGAL THEORY* 75 (1999); see also JAMES B. RULE, *PRIVATE LIVES AND PUBLIC SURVEILLANCE* 28 (1974) (finding both large-scale and less formal surveillance to be helpful to a government "or any other agency seeking to obtain compliance from a mass clientele in a large-scale social setting").

⁶⁵ JOHN GILLIOM, *OVERSEERS OF THE POOR: SURVEILLANCE, RESISTANCE, AND THE LIMITS OF PRIVACY* 3 (2001).

work of over four million public surveillance cameras—is widely perceived as “a friendly eye in the sky, not Big Brother but a kindly and watchful uncle or aunt.”⁶⁶

Too much social control, however, can adversely impact freedom, creativity, and self-development. According to Julie Cohen, “pervasive monitoring of every first move or false start will, at the margin, incline choices toward the bland and the mainstream.”⁶⁷ Monitoring constrains the “acceptable spectrum of belief and behavior,” and it results in “a subtle yet fundamental shift in the content of our character, a blunting and blurring of rough edges and sharp lines.”⁶⁸ Surveillance thus “threatens not only to chill the expression of eccentric individuality, but also, gradually, to dampen the force of our aspirations to it.”⁶⁹ Similarly, Paul Schwartz argues that surveillance inhibits freedom of choice, impinging upon self-determination.⁷⁰

In many instances, people are not directly aware that they are being observed. Does covert surveillance cause a problem? Under one view, surveillance is a *prima facie* wrong, whether overt or covert, for it demonstrates a lack of respect for its subject as an autonomous person. Philosopher Stanley Benn explains that overt surveillance does so by threatening its target’s “consciousness of pure freedom as subject, as originator and chooser.”⁷¹ As Benn contends, “[f]inding oneself an object of scrutiny, as the focus of another’s attention, brings one to a new consciousness of oneself, as something seen through another’s eyes.”⁷² Turning to covert observation, Benn explains that it “is objectionable because it deliberately deceives a person about his world, thwarting, for reasons that *cannot* be his reasons, his attempts to make a rational choice.”⁷³

Although concealed spying is certainly deceptive, Benn’s argument is unconvincing. It is the awareness that one is being watched that affects one’s freedom, and Benn fails to explain why covert surveillance has any palpable effect on a person’s welfare or activities. A more compelling reason why covert surveillance is problematic is that it can have a chilling ef-

⁶⁶ JEFFREY ROSEN, *THE NAKED CROWD: RECLAIMING SECURITY AND FREEDOM IN AN ANXIOUS AGE* 36 (2004).

⁶⁷ Cohen, *supra* note 28, at 1426.

⁶⁸ *Id.*

⁶⁹ *Id.*

⁷⁰ See Schwartz, *supra* note 18, at 1656 (“[P]erfected surveillance of naked thought’s digital expression short-circuits the individual’s own process of decisionmaking.”).

⁷¹ Stanley I. Benn, *Privacy, Freedom, and Respect for Persons*, in *NOMOS XIII: PRIVACY* 1, 7 (J. Roland Pennock & John W. Chapman eds., 1971).

⁷² *Id.*

⁷³ *Id.* at 10.

What?

* nice

fect on behavior. In fact, there can be an even greater chilling effect when people are generally aware of the possibility of surveillance, but are never sure if they are being watched at any particular moment. This phenomenon is known as the Panoptic effect, based on Jeremy Bentham's 1791 architectural design for a prison called the Panopticon.⁷⁴ The prison was set up with the inmates' cells arrayed around a central observation tower. Most importantly, the guards could see each prisoner from the tower, but the prisoners could not see the guards from their cells.⁷⁵ In Michel Foucault's words, the cells were akin to "small theatres, in which each actor is alone, perfectly individualized and constantly visible."⁷⁶ The prisoner's "only rational option" was to conform with the prison's rules because, at any moment, it was possible that they were being watched.⁷⁷ Thus, awareness of the possibility of surveillance can be just as inhibitory as actual surveillance.

neat!

One might attempt to imagine surveillance so covert that its subjects are completely unaware of even the possibility of being observed. While such well-concealed surveillance might eliminate the potential for any discomfort or chilling effect, it would still enable the watchers to gather a substantial degree of information about people, creating an architectural problem.⁷⁸ Surveillance is a sweeping form of investigatory power. It extends beyond a search, for it records behavior, social interaction, and potentially everything that a person says and does. Rather than targeting specific information, surveillance can ensnare a significant amount of data beyond any originally sought. If watched long enough, a person might be caught in some form of illegal or immoral activity, and this information could then be used to discredit or blackmail her. A prime example is the FBI's extensive wiretapping of Martin Luther King, Jr., widely believed to have been initiated in order to expose King's alleged communist ties. Though the surveillance failed to turn up any evidence of such ties, it did reveal King's extramarital affairs. The FBI then attempted to blackmail King with the information, and FBI officials leaked it in order to discredit King.⁷⁹

The law addresses surveillance, but does so by focusing on where surveillance takes place rather than on its problematic effects. The law often

⁷⁴ DAVID LYON, *THE ELECTRONIC EYE: THE RISE OF SURVEILLANCE SOCIETY* 62-67 (1994).

⁷⁵ *Id.* at 62-63.

⁷⁶ MICHEL FOUCAULT, *DISCIPLINE AND PUNISH* 200 (Alan Sheridan trans., Vintage Books, 2d ed. 1995) (1977).

⁷⁷ LYON, *supra* note 74, at 63.

⁷⁸ See *supra* note 40 and accompanying text.

⁷⁹ SOLOVE, *THE DIGITAL PERSON*, *supra* note 40, at 185. For a more extensive account of King's experience with the FBI, see DAVID J. GARROW, *THE FBI AND MARTIN LUTHER KING, JR.* (1981).

recognizes surveillance as a harm in private places but rarely in public places. In Fourth Amendment law, courts frequently conclude that surveillance in private places implicates a reasonable expectation of privacy whereas surveillance in public places does not. In *Kyllo v. United States*, the Court concluded that the Fourth Amendment required a warrant in order to use a thermal-imaging device to detect heat patterns emanating from a person's home.⁸⁰ The Court's holding relied heavily on the fact that, though conducted outside the petitioner's home, the surveillance was capturing information about activities within it: "We have said that the Fourth Amendment draws a firm line at the entrance of the house."⁸¹

When surveillance occurs in a public place, however, the Court has refused to recognize a reasonable expectation of privacy. In *Florida v. Riley*, the police flew over the defendant's greenhouse in a helicopter at four hundred feet and peered down through a few missing roof panels to observe that he was growing marijuana.⁸² The Court concluded that the defendant lacked a reasonable expectation of privacy: "As a general proposition, the police may see what may be seen from a public vantage point where [they have] a right to be."⁸³ In *Dow Chemical Co. v. United States*, the Court held that the government could not only fly over the petitioner's property and observe it with the naked eye, but could also use a powerful aerial mapping camera that enabled the identification of objects as small as one-half inch in diameter.⁸⁴

The contrast between the law's approach to surveillance in private and in public is most evident in a pair of Supreme Court cases involving location-tracking devices. In *United States v. Karo*, the Court concluded that a tracking device that monitored a person's movements within his home implicated that person's reasonable expectation of privacy.⁸⁵ In contrast, in *United States v. Knotts*, the police placed a tracking device in a can of chloroform, which the defendant then purchased and placed in his car.⁸⁶ Using the device, the police tracked the location of the defendant's vehicle.⁸⁷ According to the Court, the surveillance "amounted principally to the follow-

⁸⁰ 533 U.S. 27, 40 (2001).

⁸¹ *Id.* (internal quotation marks omitted); see also Andrew E. Taslitz, *The Fourth Amendment in the Twenty-First Century: Technology, Privacy, and Human Emotions*, 65 LAW & CONTEMP. PROBS. 125, 144 (2002) ("Central to the Court's reasoning was that the thermal imager revealed information concerning activities inside the home.").

⁸² 488 U.S. 445, 448-49 (1989).

⁸³ *Id.* at 449 (alteration in original) (internal quotation marks omitted).

⁸⁴ 476 U.S. 227, 238-39 (1986).

⁸⁵ 468 U.S. 705, 714 (1984).

⁸⁶ 460 U.S. 276, 277 (1983).

⁸⁷ *Id.*

ing of an automobile on public streets and highways.”⁸⁸ The Court concluded that the Fourth Amendment did not apply because “[a] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another.”⁸⁹ Therefore, the Court has concluded that while the Fourth Amendment protects against surveillance in private places such as one’s home, the Amendment has little applicability to surveillance in public places.⁹⁰ This understanding of privacy stems from what I call the “secrecy paradigm.”⁹¹ Under the secrecy paradigm, privacy is tantamount to complete secrecy, and a privacy violation occurs when concealed data is revealed to others. If the information is not previously hidden, then no privacy interest is implicated by the collection or dissemination of the information. In many areas of law, this narrow view of privacy has limited the recognition of privacy violations.

Tort law is generally consistent with this approach. Courts have applied the tort of intrusion upon seclusion, which protects against intrusion “upon the solitude or seclusion of another or his private affairs or concerns,”⁹² to surveillance of private places. In *Hamberger v. Eastman*, for example, the court concluded that a couple had a valid intrusion claim against their landlord for his installation of a hidden recording device in their bedroom.⁹³ In contrast, plaintiffs bringing claims involving surveillance in public have generally not been successful.⁹⁴

I think this
is somewhat
unfortunate

⁸⁸ *Id.*

⁸⁹ *Id.* at 281.

⁹⁰ See, e.g., Marc Jonathan Blitz, *Video Surveillance and the Constitution of Public Space: Fitting the Fourth Amendment to a World That Tracks Image and Identity*, 82 TEX. L. REV. 1349, 1357 (2004) (“[C]ontemporary Fourth Amendment jurisprudence differentiates pervasive video surveillance from more familiar mass suspicionless searches in one crucial respect: by holding that it is not a ‘search’ at all.”); cf. Christopher Slobogin, *Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity*, 72 MISS. L.J. 213, 233 (2002) (“Meaningful legal strictures on government use of public surveillance cameras in Great Britain, Canada, and the United States are non-existent.”).

⁹¹ SOLOVE, THE DIGITAL PERSON, *supra* note 40, at 42-44.

⁹² RESTATEMENT (SECOND) OF TORTS § 652B (1977).

⁹³ 206 A.2d 239, 241-42 (N.H. 1964); see also *Wolfson v. Lewis*, 924 F. Supp. 1413, 1431 (E.D. Pa. 1996) (finding media surveillance of a couple’s activities in their home to be actionable under intrusion tort); *Rhodes v. Graham*, 37 S.W.2d 46, 47 (Ky. 1931) (holding that wiretapping a person’s phone gives rise to a tort action because it violates his right “to the privacy of his home as against the unwarranted invasion of others”).

⁹⁴ See, e.g., *Furman v. Sheppard*, 744 A.2d 583, 586 (Md. Ct. Spec. App. 2000) (holding that the defendant was not liable under intrusion tort for trespassing into a private club to engage in video surveillance of the plaintiff because the club was not a secluded place); *Forster v. Manchester*, 189 A.2d 147, 149-50 (Pa. 1963) (finding no intrusion liability when a private investigator followed and filmed the plaintiff because the surveillance was conducted in public).

In some cases, however, courts have recognized a harm in public surveillance. For example, in *Nader v. General Motors Corp.*, Ralph Nader charged that General Motors's automobiles were unsafe.⁹⁵ General Motors undertook a massive investigation seeking information discrediting Nader. Among other things, General Motors wiretapped his telephone and placed him under extensive surveillance while in public.⁹⁶ The court recognized that certain kinds of public surveillance might amount to an invasion of privacy; although observation "in a public place does not amount to an invasion of . . . privacy," in certain instances, "surveillance may be so 'overzealous' as to render it actionable."⁹⁷ The court noted: "A person does not automatically make public everything he does merely by being in a public place, and the mere fact that Nader was in a bank did not give anyone the right to try to discover the amount of money he was withdrawing."⁹⁸ The majority reasoned that extensive public surveillance can reveal hidden details that would not ordinarily be observed by others.⁹⁹ The court's analysis, however, focused more on the harm of disclosure than on that of surveillance; pervasive surveillance could reveal details people ordinarily conceal, and thus result in the discovery of secrets.¹⁰⁰ The court did not recognize the surveillance as a harm itself—only surveillance that destroyed secrecy represented an actionable harm.¹⁰¹

Therefore, although the law often focuses on whether surveillance occurs in a public or private place, surveillance is harmful in all settings, not just private ones.¹⁰² Surveillance in public can certainly cause uneasiness, as illustrated by the example of being stared at continuously in public. As Alan Westin observes: "Knowledge or fear that one is under systematic observation in public places destroys the sense of relaxation and freedom that men seek in open spaces and public arenas."¹⁰³ Moreover, public surveillance can have chilling effects that make people less likely to associate with

⁹⁵ 225 N.E.2d 765, 767 (N.Y. 1970).

⁹⁶ *Id.*

⁹⁷ *Id.* at 771.

⁹⁸ *Id.*

⁹⁹ *Id.* at 769.

¹⁰⁰ *Id.* at 768-69.

¹⁰¹ *Id.* at 771 ("On the other hand, if the plaintiff acted in such a way as to reveal that fact to any casual observer, then, it may not be said that the appellant intruded into his private sphere.").

¹⁰² See ABA CRIMINAL JUSTICE SECTION'S STANDARDS COMM., ABA CRIMINAL JUSTICE STANDARDS ON ELECTRONIC SURVEILLANCE RELATING TO TECHNOLOGICALLY-ASSISTED PHYSICAL SURVEILLANCE § 2-6.1(d) to (g) (Draft 3d ed. 1997) (recommending that the law begin to address the harms of public surveillance).

¹⁰³ WESTIN, *supra* note 19, at 31.

certain groups, attend rallies, or speak at meetings.¹⁰⁴ Espousing radical beliefs and doing unconventional things takes tremendous courage; the attentive gaze, especially the government's, can make these acts seem all the more daring and their potential risks all the more inhibitory. Thus, the dignitary harms and architectural problems of surveillance can occur both in public and private places. The law, however, tends to focus more on secrecy than on the particular problems and harms caused by surveillance.

2 Interrogation

The Fifth Amendment provides that "[n]o person . . . shall be compelled in any criminal case to be a witness against himself."¹⁰⁵ The Amendment creates a "privilege against self-incrimination," and it prevents the government from compelling individuals to testify against themselves.¹⁰⁶ The privilege has been justified as protecting against "[t]he essential and inherent cruelty of compelling a man to expose his own guilt,"¹⁰⁷ as "a safeguard of conscience and human dignity,"¹⁰⁸ and as promoting "respect for personal integrity."¹⁰⁹

What is so inhumane about having to answer the government's questions about one's criminal acts? Why do we want to protect a potentially guilty person from having to divulge her criminal activities?

A different, less coercive form of interrogation occurs when others or the government ask questions for purposes other than criminal prosecution. In the late nineteenth century, there was a loud public outcry when the U.S. census began including more and more questions relating to personal affairs, such as marital status, literacy, property ownership, health, and finances.¹¹⁰ In the 1870s, an editorial in *The New York Times*, as well as editorials in other papers, decried the "inquisitorial" nature of the census.¹¹¹ A poem in *The New York Sun* in 1890 humorously criticized the census:

¹⁰⁴ As Justice Douglas observed in another case: "Monitoring, if prevalent, certainly kills free discourse and spontaneous utterances." *United States v. White*, 401 U.S. 745, 762 (1971) (Douglas, J., dissenting).

¹⁰⁵ U.S. CONST. amend. V.

¹⁰⁶ DAVID M. O'BRIEN, *PRIVACY, LAW, AND PUBLIC POLICY* 92-93 (1979) (emphasis omitted).

¹⁰⁷ *Brown v. Walker*, 161 U.S. 591, 637 (1896) (Field, J., dissenting).

¹⁰⁸ *Ullmann v. United States*, 350 U.S. 422, 445 (1956) (Douglas, J., dissenting).

¹⁰⁹ Charles Fried, *Privacy*, 77 YALE L.J. 475, 488 (1968).

¹¹⁰ See Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393, 1401 (2001).

¹¹¹ ROBERT ELLIS SMITH, *BEN FRANKLIN'S WEB SITE: PRIVACY AND CURIOSITY FROM PLYMOUTH ROCK TO THE INTERNET* 62 (2000).

I never
really got
this one.

I am a census inquisitor.
I travel about from door to door,
From house to house, from store to store,
With pencil and paper and power galore.
I do as I like and ask what I please.
Down before me you must get on your knees;
So open your books, hand over your keys,
And tell me about your chronic disease.¹¹²

Why was there such an outcry? When asked a probing question that people find unwarranted, a frequent response is a snippy reply: "None of your business!" Why do such questions evoke such a response? Why do people take offense even at being asked certain questions—let alone being compelled to answer them?

Understood broadly, these examples all involve a similar practice—what I call "interrogation." Interrogation is the pressuring of individuals to divulge information. Interrogation has many benefits; it is useful for ferreting out information that others want to know.

However, interrogation can create harm. Part of this harm arises from the degree of coerciveness involved. The Fifth Amendment privilege protects against highly coercive interrogation about matters with enormous personal stakes for the examined subject.¹¹³ However, for interrogation generally, the compulsion need not be direct; nor must it rise to the level of outright coercion. Compulsion can consist of the fear of not getting a job or of social opprobrium. People take offense when others ask an unduly probing question—even if there is no compulsion to answer. One explanation may be that people still feel some degree of compulsion because not answering might create the impression that they have something to hide. This is why, I believe, there are social norms against asking excessively probing or prying questions: they make the person being questioned feel uncomfortable. Interrogation forces people to be concerned about how they will explain themselves or how their refusal to answer will appear to others.

Interrogation resembles intrusion in its invasiveness, for interrogation is a probing, a form of searching. Like disclosure, interrogation often involves the divulging of concealed information; unlike disclosure, interrogation can create discomfort even if the information is barely disseminated. To some degree, surveillance resembles interrogation, for both involve the involuntary gathering of information. Interrogation, however, occurs with the conscious awareness of the subject; surveillance can be clandestine.

¹¹² *Id.* at 63.

¹¹³ See, e.g., *Miranda v. Arizona*, 384 U.S. 436, 467 (1966) (explaining the Fifth Amendment protections against self-incrimination in the context of custodial interrogation).

Historically, interrogation has been employed to impinge upon freedom of association and belief. During the McCarthy era in the 1950s, the House Un-American Activities Committee (HUAC) employed interrogation to attack Communists and inhibit their association and expression of political beliefs.¹¹⁴ Dissenting in *Barenblatt v. United States*, in which the Court upheld the Committee's power to force a witness to answer questions about Communist ties,¹¹⁵ Justices Black, Warren and Douglas argued that the interrogation's harm did not affect the witness alone.¹¹⁶ They spoke of interrogation impeding "the interest of the people as a whole in being able to join organizations, advocate causes and make political 'mistakes' without later being subjected to governmental penalties for having dared to think for themselves."¹¹⁷

Another aspect of the power of interrogation is its potential for resulting in distortion. The interrogator possesses extraordinary control over what information is elicited, how it is interpreted, and the impressions created by its revelations. A skillful interrogator can orchestrate a dialogue that creates impressions and inferences that she wants to elicit. In cross-examination, a skilled attorney can carefully manipulate what a witness says and can intimidate a witness into coming across less favorably. Thus, one of the rationales justifying the privilege against self-incrimination is that it protects accuracy.¹¹⁸ Even in the absence of deliberate manipulation, the interrogation process can be distorting. "The interrogat[ion]," observes Peter Brooks, "seeks to pattern the unfolding narrative according to a preconceived story."¹¹⁹ Interrogation can be distorting because information is elicited by another, often without an interest in learning the whole story. In questionnaires and standardized forms, for example, distortion creeps in because the questions often do not ask for the entire story or are phrased in certain ways that yield deceptive results.

¹¹⁴ ELLEN SCHRECKER, *MANY ARE THE CRIMES: MCCARTHYISM IN AMERICA* 369-70 (1998).

¹¹⁵ 360 U.S. 109, 127, 134 (1959).

¹¹⁶ *Id.* at 144 (Black, J., dissenting).

¹¹⁷ *Id.* (emphasis added).

¹¹⁸ As Wigmore noted: "The simple and peaceful process of questioning breeds a readiness to resort to bullying and to physical force and torture." 8 JOHN HENRY WIGMORE, *EVIDENCE IN TRIALS AT COMMON LAW* § 2251 n.1(c) (John T. McNaughton ed., 4th ed. 1961).

¹¹⁹ PETER BROOKS, *TROUBLING CONFESSIONS: SPEAKING GUILT IN LAW AND LITERATURE* 40 (2000). The interrogation of Dimitri Karamazov in Fyodor Dostoevsky's *The Brothers Karamazov* is an excellent literary example of how interrogation distorts the truth even when the interrogators bear no deliberate motivation to distort. See RICHARD H. WEISBERG, *THE FAILURE OF THE WORD* 55-58 (1984) (commenting on "Dostoevsk[y]'s belief that the legal investigator, like the novelist himself, is motivated by an essentially personalized vision of reality").

Beyond the Fifth Amendment, there are numerous legal protections against interrogation. The First Amendment prevents government questioning about one's political associations. In *Shelton v. Tucker*, the Court applied strict scrutiny and struck down a law requiring public teachers to list all organizations to which they belong or contribute.¹²⁰ Later, in *Baird v. State Bar of Arizona*, the Court held that a state may not ask questions solely to gain information about a person's political views or associations.¹²¹ According to the Court: "[W]hen a State attempts to make inquiries about a person's beliefs or associations, its power is limited by the First Amendment. Broad and sweeping state inquiries into these protected areas, as Arizona has engaged in here, discourage citizens from exercising rights protected by the Constitution."¹²²

Rape shield laws restrict the questioning of rape victims in court.¹²³ The Americans with Disabilities Act of 1990 limits certain employer inquiries about employee disabilities.¹²⁴ Many states prohibit employers from questioning employees or applicants about certain matters. For example, Wisconsin forbids employers from requiring employees or applicants to undergo HIV testing.¹²⁵ Massachusetts prohibits employers from asking about arrests not leading to conviction, misdemeanor convictions, or any prior commitment to mental health treatment facilities.¹²⁶ Several states restrict employers from requiring employees or applicants to undergo genetic testing.¹²⁷ Evidentiary privileges protect communications between attorneys

¹²⁰ 364 U.S. 479, 488-90 (1960).

¹²¹ 401 U.S. 1, 6-7 (1971). If the government has other purposes for asking such information, however, questions about political views and organizations are permissible. See *Law Students Civil Rights Research Council, Inc. v. Wadmond*, 401 U.S. 154, 165-66 (1971) (remarking that questions about membership and intent to further a subversive organization's illegal aims were constitutionally proper); *Barenblatt v. United States*, 360 U.S. 109, 127-28 (1959) (holding that a person could be compelled to disclose before the House Un-American Activities Committee whether he was a member of the Communist Party because questions were related to a "valid legislative purpose").

¹²² *Baird*, 401 U.S. at 6.

¹²³ See Harriet R. Galvin, *Shielding Rape Victims in the State and Federal Courts: A Proposal for the Second Decade*, 70 MINN. L. REV. 763, 765-66 (1986) (discussing how rape shield laws reversed the common law doctrine that allowed a defendant to inquire into the complainant's tendency to engage in extramarital sexual relations).

¹²⁴ See 42 U.S.C. § 12112(d)(2) (2000) (limiting the legality of inquiries during the pre-employment period); *id.* § 12112(d)(4) (prohibiting inquiries during the employment period). Drug testing is not considered a "medical examination" under the ADA. *Id.* § 12114(d)(1).

¹²⁵ WIS. STAT. ANN. § 103.15(2) (West 2002).

¹²⁶ MASS. GEN. LAWS ANN. ch. 151B, § 4(9), (9A) (LexisNexis 1999).

¹²⁷ See, e.g., CAL. GOV'T CODE § 12940(o) (West 2005); CONN. GEN. STAT. ANN. § 46a-60(11)(A) (West 2004); DEL. CODE ANN. tit. 19, § 711(e) (Supp. 2004); N.Y. EXEC. LAW § 296.19(a)(1) (McKinney 2004).

and clients, priests and penitents, and doctors and patients.¹²⁸ Privileges do not guard against the questioning of the individual about her personal information; rather, they protect against the questioning of others about it. As Catherine Ross contends, privileges protect against "forced betrayal."¹²⁹

Although the law protects against interrogation, it does so in a complicated and unsystematic way. The Fifth Amendment's protection against interrogation is very limited. The Fifth Amendment certainly does not protect the information itself; if the same facts can be produced at trial via other witnesses or evidence, they are not prohibited. The Fifth Amendment is therefore concerned only partly with the type of information involved—its applicability turns on compelled self-disclosure. However, as William Stuntz observes, under current Fifth Amendment law:

As long as use immunity is granted, the government is free to compel even the most damning and private disclosures. . . . If the privilege were sensibly designed to protect privacy, . . . its application would turn on the nature of the disclosure the government wished to require, and yet settled fifth amendment law focuses on the criminal consequences of disclosure.¹³⁰

Incriminating information may thus be compelled even under the Fifth Amendment if there are no criminal consequences—even if the compulsion would cause a person great disgrace.¹³¹ In *Ullmann v. United States*, for example, a witness granted immunity to testify as to his activities in the Communist Party contended that he would not only suffer disgrace, but would suffer severe social sanctions as a result, including losing his job and friends, and being blacklisted from future employment.¹³² The Court rejected the witness's argument because no criminal sanctions would be imposed as a

¹²⁸ See, e.g., ARIZ. REV. STAT. ANN. § 12-2235 (2005) (privileging, in civil actions, any patient communication to a physician or surgeon regarding "any physical or mental disease or disorder or supposed physical or mental disease or disorder or as to any such knowledge obtained by personal examination of the patient"); CAL. EVID. CODE § 954 (West 1995) ("[T]he client . . . has a privilege to refuse to disclose, and to prevent another from disclosing, a confidential communication between client and lawyer . . ."); 735 ILL. COMP. STAT. ANN. 5/8-803 (West 2005) (rendering privileged any "confession or admission" made to an accredited practitioner of a religious denomination in her official capacity).

¹²⁹ Catherine J. Ross, *Implementing Constitutional Rights for Juveniles: The Parent-Child Privilege in Context*, 14 STAN. L. & POL'Y REV. 85, 86 (2003).

¹³⁰ William J. Stuntz, *Self-Incrimination and Excuse*, 88 COLUM. L. REV. 1227, 1234 (1988) (footnotes omitted).

¹³¹ See *Brown v. Walker*, 161 U.S. 591, 605-06 (1896) ("The design of the constitutional privilege [against self-incrimination] is not to aid the witness in vindicating his character, but to protect him against being compelled to furnish evidence to convict him of a criminal charge.").

¹³² 350 U.S. 422, 430 (1956).

result of his testifying.¹³³ In dissent, Justice Douglas argued that the "Fifth Amendment was designed to protect the accused against infamy as well as against prosecution," and that the "curse of infamy" could be as damaging as criminal punishment.¹³⁴ Nevertheless, Douglas's view has not been accepted in Fifth Amendment doctrine. It remains unclear what interests the Fifth Amendment protects. As Stuntz observes: "It is probably fair to say that most people familiar with the doctrine surrounding the privilege against self-incrimination believe that it cannot be squared with any rational theory."¹³⁵

Evidentiary privileges, like the Fifth Amendment, are also quite narrow in scope. Despite strong public disapproval of forcing parents and children to testify against each other, the majority of courts have rejected a parent-child privilege.¹³⁶ Still, in the words of one court, "forcing a mother and father to reveal their child's alleged misdeeds . . . is shocking to our sense of decency, fairness and propriety."¹³⁷

Privacy law's theory of interrogation is not only incoherent, it is nearly nonexistent. Despite recognizing the harms and problems of interrogation—compulsion, divulgence of private information, and forced betrayal—the law only addresses them in limited situations.

B. *Information Processing*

Information processing refers to the use, storage, and manipulation of data that has been collected. Information processing does not involve the collection of data; rather, it concerns how already-collected data is handled.

¹³³ *Id.* at 439.

¹³⁴ *Id.* at 450, 452 (Douglas, J., dissenting).

¹³⁵ Stuntz, *supra* note 130, at 1228.

¹³⁶ See *In re Grand Jury*, 103 F.3d 1140, 1146 (3d Cir. 1997) ("The overwhelming majority of all courts—federal or state—have rejected such a privilege.").

¹³⁷ *In re A & M*, 403 N.Y.S.2d 375, 380 (App. Div. 1978). When Monica Lewinsky's mother was subpoenaed to testify against her by Independent Counsel Ken Starr in his investigation of President Bill Clinton, there was an enormous public outcry. See Ruth Marcus, *To Some in the Law, Starr's Tactics Show a Lack of Restraint*, WASH. POST, Feb. 13, 1998, at A1 (providing reactions from prosecutors who believed Starr's tactics were unwarranted). Critics have likened the tactic of having parents and children testify about each other to some of the infamous horrors of totalitarian societies, such as Nazi Germany, where the government sought to make family members divulge information about each other. See, e.g., J. Tyson Covey, *Making Form Follow Function: Considerations in Creating and Applying a Statutory Parent-Child Privilege*, 1990 U. ILL. L. REV. 879, 890 (postulating that recognition of some form of a parent-child privilege would help to prevent the state from forcing children and parents into a troubling predicament); Wendy Meredith Watts, *The Parent-Child Privileges: Hardly a New or Revolutionary Concept*, 28 WM. & MARY L. REV. 583, 590-94 (1987) (noting that parent-child privileges are not recognized in despotic regimes).

I will discuss five forms of information processing: (1) aggregation, (2) identification, (3) insecurity, (4) secondary use, and (5) exclusion.

Processing involves various ways of connecting data together and linking it to the people to whom it pertains. Even though it can involve the transmission of data, processing diverges from dissemination because the data transfer does not involve the disclosure of the information to the public—or even to another person. Rather, data is often transferred between various record systems and consolidated with other data. Processing diverges from information collection because processing creates problems through the consolidation and use of the information, not through the means by which it is gathered.

1. Aggregation

The rising use of computers in the 1960s raised public concern about privacy.¹³⁸ Commentators devoted significant attention to the issue,¹³⁹ and privacy became an important topic on Congress's agenda.¹⁴⁰ Significant concern was devoted to the data maintained by the federal government. In 1965, a group of academics led by professor Richard Ruggles criticized the fact that the government's data systems were decentralized and recommended consolidation.¹⁴¹ The Bureau of the Budget (now called the Office of Management and Budget) supported the idea and suggested the creation

¹³⁸ REGAN, *supra* note 43, at 82.

¹³⁹ See, e.g., MYRON BRENTON, *THE PRIVACY INVADERS* 13 (1964) (discussing how life in the 1960s brings with it some compulsory encroachments on privacy, but that "'reasonable' encroachments are fast becoming unreasonable . . . invasions . . . tending to make intrusion a way of everyday life" (emphasis omitted)); MILLER, *supra* note 5, at ix-x (discussing "the profound effect computer technology is certain to have on numerous facets of the law" including individual privacy); VANCE PACKARD, *THE NAKED SOCIETY* 12 (1964) ("Today it is increasingly assumed that the past and present of all of us . . . must be an open book; and that all such information about us can be not only put in files but merchandised freely."); WESTIN, *supra* note 19, at 3 (arguing that society needs to "move from public awareness of the problem to a sensitive discussion of what can be done to protect privacy in an age when so many forces of science [and] technology . . . press against it from all sides"); Kenneth L. Karst, "The Files": *Legal Controls over the Accuracy and Accessibility of Stored Personal Data*, 31 *LAW & CONTEMP. PROBS.* 342, 343 (1966) (identifying two problems arising from the maintenance and usage of computerized personal data files—"access and accuracy" of information—which "raise divergent questions for the legal system"); Symposium, *Computers, Data Banks, and Individual Privacy*, 53 *MINN. L. REV.* 211-45 (1968) (exploring the possibility and danger of National Data Banks, including personal privacy implications).

¹⁴⁰ See REGAN, *supra* note 43, at 82 (reporting that Congress held many hearings on the issue in the late 1960s and early 1970s).

¹⁴¹ SMITH, *supra* note 111, at 309.

of a Federal Data Center.¹⁴² The plan was quickly attacked in Congress and scrapped.¹⁴³ In 1974, the General Services Administration proposed the creation of FEDNET, a plan to link together all computer systems maintained by the federal government.¹⁴⁴ Vice President Ford immediately halted the plan.¹⁴⁵

What was the concern? The data was already in the record systems of government agencies. Why was it a problem for the government to combine it into one gigantic database?

The problem is one that I have called "aggregation."¹⁴⁶ Aggregation is the gathering together of information about a person. A piece of information here or there is not very telling. But when combined together, bits and pieces of data begin to form a portrait of a person. The whole becomes greater than the parts.¹⁴⁷ This occurs because combining information creates synergies. When analyzed, aggregated information can reveal new facts about a person that she did not expect would be known about her when the original, isolated data was collected.

Aggregating information is certainly not a new activity. It was always possible to combine various pieces of personal information, to put two and two together to learn something new about a person. But aggregation's power and scope are different in the Information Age; the data gathered about people is significantly more extensive, the process of combining it is much easier, and the computer technologies to analyze it are more sophisticated and powerful.

Combining data and analyzing it certainly can be put to beneficial uses. Amazon.com, for example, uses aggregated data about a person's book-buying history to recommend other books that the person might find of interest. Credit reporting allows creditors to assess people's financial reputations in a world where first-hand experience of the financial condition and trustworthiness of individuals is often lacking.¹⁴⁸ These developments make

I don't
see the
problem

¹⁴² *Id.* at 310-11. But cf. Note, *Privacy and Efficient Government: Proposals for a National Data Center*, 82 HARV. L. REV. 400, 412 (1968) (criticizing the congressional task force for undertaking "only a surface treatment" of the privacy issue and arguing that "Congress should give very careful consideration to essential legal and technological safeguards for the privacy interest").

¹⁴³ SMITH, *supra* note 111, at 311.

¹⁴⁴ *Id.*

¹⁴⁵ *Id.*

¹⁴⁶ SOLOVE, *THE DIGITAL PERSON*, *supra* note 40, at 44-47.

¹⁴⁷ See Cohen, *supra* note 28, at 1398 ("A comprehensive collection of data about an individual is vastly more than the sum of its parts.")

¹⁴⁸ See STEVEN L. NOCK, *THE COSTS OF PRIVACY: SURVEILLANCE AND REPUTATION IN AMERICA* 73 (1993) (noting that "in a society of strangers . . . so much depends on the faith

sense in a world where there are billions of people and word-of-mouth is insufficient to assess reputation.

Alongside these benefits, however, aggregation can cause dignitary harms because of how it unsettles expectations. People expect certain limits on what is known about them and on what others will find out. Aggregation upsets these expectations, because it involves the combination of data in new, potentially unanticipated ways to reveal facts about a person that are not readily known. People give out bits of information in different settings, only revealing a small part of themselves in each context. Indeed, people selectively spread around small pieces of data throughout most of their daily activities, and they have the expectation that in each disclosure, they are revealing relatively little about themselves. When these pieces are consolidated together, however, the aggregator acquires much greater knowledge about the person's life.

Like surveillance, aggregation is a way to acquire information about people. It reveals facts about data subjects in ways far beyond anything they expected when they gave out the data. However, aggregation is a less direct form of data acquisition than surveillance, for it occurs through processing data already gathered from individuals.

Aggregation can also lead to architectural problems; it can increase the power that others have over individuals. The dossier created by aggregating a person's data is often used as a way to judge her. Aggregations of data, such as credit reports, are used to evaluate data about a person's financial reputation and then make decisions that profoundly affect a person's life, including whether she gets a loan, a lease, or a mortgage. Elsewhere, I have discussed the multitude of ways that the compilation of an individual's data—what I call the “digital person”—is being used to make important decisions about an individual. The digital person in digital space increasingly is affecting the flesh-and-blood individual in realspace.¹⁴⁹

Although making decisions based on aggregated data is efficient, it also creates problems. Data compilations are often both telling and incomplete. They reveal facets of our lives, but the data is often reductive and disconnected from the original context in which it was gathered. This leads to distortion. As H. Jeff Smith observes:

[D]ecisions that were formerly based on judgment and human factors are instead often decided according to prescribed formulas. In today's world, this response is often characterized by reliance on a rigid, unyielding process in

we have in one another's truthfulness,” and that “[l]acking the personal information necessary to discern the veracity of others' claims, we trust instead the monitoring provided by large social structures” and institutions such as credit bureaus).

¹⁴⁹ SOLOVE, *THE DIGITAL PERSON*, *supra* note 40, at 1-10.

bt I want
to could be
able to plate
my address...

X
that I see

bt not for go

which computerized information is given great weight. Facts that actually require substantial evaluation could instead be reduced to discrete entries in pre-assigned categories.¹⁵⁰

Some courts have recognized aggregation as violating a privacy interest. In *United States Department of Justice v. Reporters Committee for Freedom of the Press*, the Supreme Court concluded that the disclosure of FBI "rap sheets" was an invasion of privacy within a privacy exemption of the Freedom of Information Act (FOIA).¹⁵¹ Pursuant to FOIA, "any person" may request "records" maintained by an executive agency.¹⁵² The rap sheets contained extensive information about individuals compiled from a variety of criminal records.¹⁵³ FOIA exempts law enforcement records that "could reasonably be expected to constitute an unwarranted invasion of personal privacy."¹⁵⁴ Although the reporters argued that the rap sheets were not private because all of the information in them had already been disclosed, the Court disagreed, noting that in "an organized society, there are few facts that are not at one time or another divulged to another."¹⁵⁵ Thus, the Court observed, there is a "distinction, in terms of personal privacy, between scattered disclosure of the bits of information contained in a rap sheet and revelation of the rap sheet as a whole."¹⁵⁶

Reporters Committee is one of the rare instances where the law has recognized that aggregation can make a material difference in what is known about an individual. Most courts adhere to the secrecy paradigm, which fails to recognize any privacy interest in information publicly available or already disseminated to others.¹⁵⁷ The Restatement of Torts declares that for the tort of publicity given to private life, "[t]here is no liability when the defendant merely gives further publicity to information about the plaintiff that is already public. Thus there is no liability for giving publicity to facts about the plaintiff's life that are matters of public record."¹⁵⁸ Similarly, the Restatement provides that for the tort of intrusion upon seclusion, "there is

¹⁵⁰ H. JEFF SMITH, *MANAGING PRIVACY: INFORMATION TECHNOLOGY AND CORPORATE AMERICA* 121 (1994) (footnote omitted).

¹⁵¹ 489 U.S. 749, 780 (1989).

¹⁵² 5 U.S.C. § 552(a)(3)(A) (2000).

¹⁵³ *Reporters Comm.*, 489 U.S. at 749.

¹⁵⁴ 5 U.S.C. § 552(b)(7)(C).

¹⁵⁵ *Reporters Comm.*, 489 U.S. at 763.

¹⁵⁶ *Id.* at 764.

¹⁵⁷ See, e.g., *Cordell v. Detective Publ'ns*, 307 F. Supp. 1212, 1218 (E.D. Tenn. 1968) ("The Court is of the opinion that the plaintiff may not complain of public disclosure of private facts when the material facts [of concern] are not private but are matters of public record and are in the public domain.").

¹⁵⁸ RESTATEMENT (SECOND) OF TORTS § 652D cmt. b (1965).

that seemed
a bit arbitrary

lib posting
public records
online

no liability for the examination of a public record concerning the plaintiff."¹⁵⁹ In contrast, aggregation would violate a privacy interest when the aggregation significantly increases what others know about a person, even if originating from public sources.

Differing from *Reporters Committee*, courts have refused to find privacy interests in compilations of information disclosed in Megan's Laws, which involve the dissemination of personal data about convicted sex-offenders.¹⁶⁰ In *Russell v. Gregoire*, the court rejected a constitutional challenge to Washington's Megan's Law because the information was not private since it was "already fully available to the public."¹⁶¹ Similarly, in *Paul P. v. Verniero*, the Court declined to follow *Reporters Committee* in concluding that New Jersey's Megan's Law was constitutional.¹⁶² As one court observed: "Both the Third Circuit and this Court have repeatedly stressed that *Reporters Committee* is inapposite on the issue of those privacy interests entitled to protection under the United States Constitution."¹⁶³ These cases limited *Reporters Committee* to the FOIA context, but they did not supply a reason why recognizing a privacy interest in aggregated data is necessarily linked only to FOIA and does not apply to other areas of law. Legally, the cases have drawn a line, but conceptually, no justification has been offered for the limitation.

Of course, there are many reasons why Megan's Laws might outweigh privacy interests—namely, as a means to promote safety of children, to keep parents informed of which neighbors to avoid, and to help parents make sure that the babysitter they hired is not a prior child molester. However, *Russell*¹⁶⁴ and *Paul P.*¹⁶⁵ did not recognize a privacy interest in the aggregated data, and thus no balancing took place between this privacy interest and the safety interest.

Yeah
Same case
diff outcome

¹⁵⁹ *Id.* § 652B cmt. c.

¹⁶⁰ See, e.g., *Cutshall v. Sundquist*, 193 F.3d 466, 481 (6th Cir. 1999) (concluding that *Reporters Committee* was not applicable to a Megan's Law challenge). But see *Doe v. Poritz*, 662 A.2d 367, 411 (N.J. 1995) (following *Reporters Committee* and recognizing a privacy interest with respect to a sex offender community-notification statute).

¹⁶¹ 124 F.3d 1079, 1094 (9th Cir. 1997).

¹⁶² 170 F.3d 396, 400, 405 (3d Cir. 1999), *aff'd on reh'g sub nom.* *Paul P. v. Farmer*, 227 F.3d 98 (3d Cir. 2000) (stating that the holding of *Reporters Committee* dealt with the implication of a privacy interest protected by an exemption to the Freedom of Information Act, not by the Constitution, as in the case of *Paul P.*).

¹⁶³ A.A. v. New Jersey, 176 F. Supp. 2d 274, 305 (D.N.J. 2001), *aff'd* 341 F.3d 206 (3d Cir. 2003).

¹⁶⁴ 124 F.3d at 1094.

¹⁶⁵ 170 F.3d at 405.

2. Identification

Although proposed many times in the United States, a national identification card has been explicitly rejected. When the Social Security System was first developed, "President Roosevelt and members of Congress promised that the Social Security card would be kept confidential and would not be used for identification purposes."¹⁶⁶ The cards even stated that they were "not for identification."¹⁶⁷ In 1973, the influential report, *Records, Computers, and the Rights of Citizens*, concluded:

We take the position that a standard universal identifier (SUI) should not be established in the United States now or in the foreseeable future. By our definition, the Social Security Number (SSN) cannot fully qualify as an SUI; it only approximates one. However, there is an increasing tendency for the Social Security number to be used as if it were an SUI.¹⁶⁸

data problems

Why were there strong negative reactions to identification systems? What is the problem with identifying people?

"Identification" is connecting information to individuals. According to Roger Clarke, identification is "the association of data with a particular human being."¹⁶⁹ Identification enables us to attempt to verify identity—that the person accessing her records is indeed the owner of the account or the subject of the records. Identification enables us not only to confirm the identity of a person, but also to discover the perpetrator of a crime from traces left behind, such as fingerprints and genetic material.¹⁷⁰

Identification is related to disclosure in that both involve the revelation of true information. Identification involves a particular form of true information (one's identity), which enables databases of information to be linked to people. Identification is similar to aggregation as both involve the combination of different pieces of information, one being the identity of a person. However, identification differs from aggregation in that it entails a link

¹⁶⁶ Richard Sobel, *The Demeaning of Identity and Personhood in National Identification Systems*, 15 HARV. J.L. & TECH. 319, 349-50 (2002) (footnote omitted).

¹⁶⁷ *Id.* at 350.

¹⁶⁸ U.S. DEP'T OF HEALTH, EDUC., & WELFARE, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS xxxii (1973).

¹⁶⁹ ROGER CLARKE, SMART CARD TECHNICAL ISSUES STARTER KIT, ch. 3 (April 8, 1998), available at <http://www.anu.edu.au/people/Roger.Clarke/DV/SCTISK3.html>. As Clarke observes: "In the context of information systems, the purpose of identification is more concrete: it is used to link a stream of data with a person." Roger Clarke, *Human Identification in Information Systems: Management Challenges and Public Policy Issues*, 7 INFO. TECH. & PEOPLE 6, 8 (1994), available at <http://www.anu.edu.au/people/Roger.Clarke/DV/HumanID.html> [hereinafter Clarke, *Information Systems*].

¹⁷⁰ For a history of criminal identification techniques, see SIMON A. COLE, SUSPECT IDENTITIES: A HISTORY OF FINGERPRINTING AND CRIMINAL IDENTIFICATION 4-5 (2001).

to the person in the flesh. For example, there can be extensive aggregations of data about a person in many databases, but these aggregations might be rarely connected to that person as she goes through her day-to-day activities. This is a situation involving high aggregation and low identification. On the flip side, one can have high identification and low aggregation, such as in a world of checkpoints, where people constantly have to show identification but where there are few linkages to larger repositories of data about people.

Identification has many benefits.¹⁷¹ In order to access various accounts, people's identity must be verified, a step that can reduce fraud and enhance accountability. Identification can deter misleading political campaign ads. Under federal election law, television ads advocating the election or defeat of a candidate must identify the person or group placing the ad.¹⁷² If an ad is not authorized by a candidate, it "shall clearly state the name and permanent street address, telephone number, or World Wide Web address of the person who paid for the communication and state that the communication is not authorized by any candidate or candidate's committee."¹⁷³ Identification requirements such as this one can help prevent misinformation and enable people to better assess the ad.

Although identification of people or sources of particular messages can be beneficial, it also creates problems. There are some who argue that identification is demeaning to dignity because it reduces people to a number or to bodily characteristics.¹⁷⁴ But, identification is a means to link people to data, not necessarily an indication that people are the equivalent of their identifying characteristics. One need not assume that identification equates individual identity with the identifiers. Therefore, I do not agree that identification is inherently demeaning to dignity.

There is, nonetheless, a more compelling argument for why identification can negatively impact identity. The problem stems not from the identifier itself but from how it links data to individuals. Because it connects people to data, identification attaches informational baggage to people. This

¹⁷¹ See generally JOHN D. WOODWARD, JR. ET AL., *BIOMETRICS: IDENTITY ASSURANCE IN THE INFORMATION AGE* (2003) (commenting that reliable identification improves public safety and the safety of business transactions).

¹⁷² See Communications Disclaimer Requirements, 11 C.F.R. § 110.11 (2005) (requiring disclaimers on "general public political advertising"). The identification requirement was originally part of the Federal Election Campaign Act of 1971, Pub. L. No. 92-225, 86 Stat. 3 (1972) (codified as amended at 2 U.S.C. §§ 431-456 (2000 & Supp. II 2002)), which required identification for any expenditure with the purpose of influencing an election. The Court in *Buckley v. Valeo* held that the provision can only apply to speech that "expressly advocate[s] the election or defeat of a clearly identified candidate." 424 U.S. 1, 79-80 (1976).

¹⁷³ 2 U.S.C. § 441d(a)(3) (2000 & Supp. II 2002).

¹⁷⁴ See Clarke, *Information Systems*, *supra* note 169, at 32-34 (describing proponents of this view).

That's why
we connect it
in a very hit+
miss way
that leads
to 'identity
fraud

pointer!

alters what others learn about people as they engage in various transactions and activities. An interesting example of this was a case before the European Court of Human Rights (ECHR), which enforces the Council of Europe's Convention for the Protection of Human Rights and Fundamental Freedoms.¹⁷⁵ In *B. v. France*, a French citizen who had surgically changed her sex from male to female sought to have her identification documents (birth certificate, identity card, passport, and voting card) changed from listing her former male name to a female one.¹⁷⁶ Since gender was "indicated on all documents using the identification number issued to everyone" and since this "number was used as part of the system of dealings between social security institutions, employers and those insured," it prevented her from concealing the fact she was a transsexual and effectively assuming a female identity.¹⁷⁷ As the Commission stated:

A transsexual was consequently unable to hide his or her situation from a potential employer and the employer's administrative staff; the same applied to the many occasions in daily life where it was necessary to prove the existence and amount of one's income (taking a lease, opening a bank account, applying for credit, etc.). This led to difficulties for the social and professional integration of transsexuals.¹⁷⁸

The Commission concluded that the applicant, "as a result of the frequent necessity of disclosing information concerning her private life to third parties, suffered distress which was too serious to be justified on the ground of respect for the rights of others."¹⁷⁹ This case illustrates how identification can inhibit people's ability to change and can prevent their self-development by tying them to a past from which they want to escape.¹⁸⁰

In some ways, identification resembles interrogation, as identification often involves the questioning of individuals to compel them to identify themselves. Identification is a component of certain forms of surveillance insofar as it facilitates the detection and monitoring of a person and enables surveillance data to be categorized according to the individuals to which it pertains.

¹⁷⁵ Article 8 of the Convention provides for the protection of "the right to respect for [an individual's] private and family life, his home and his correspondence." Convention for the Protection of Human Rights and Fundamental Freedoms art. 8, Nov. 4, 1950, 213 U.N.T.S. 221.

¹⁷⁶ 232 Eur. Ct. H.R. 33, 36 (1992).

¹⁷⁷ *Id.* at 52.

¹⁷⁸ *Id.*

¹⁷⁹ *Id.*

¹⁸⁰ The science fiction movie *Gattaca* also illustrates these points. Vincent, the protagonist, is linked to his high risk of developing heart problems, thus rendering him unfit for all but the most menial of jobs. *GATTACA* (Columbia Pictures 1997).

Identification is thus interrelated with other forms of privacy disruption, and, like those forms, it reveals, distorts, and intrudes. Identification diverges, however, because it is primarily a form of connecting data to people. Aggregation creates what I have called a "digital person," a portrait composed of information fragments combined together.¹⁸¹ Identification goes a step further—it links the digital person directly to a person in realspace.

Some forms of identification can have similar effects to disclosure. For example, expressive methods of identification, such as branding, tattooing, or scarlet letters have been used "usually in the context of slavery, racial subjugation or harsh criminal systems."¹⁸² The identification marker conveys certain information and often bears a particular stigma. In contrast, nonexpressive means of identification, such as fingerprints, identify people without signaling anything to the public.

Identification also creates architectural problems, for it increases the government's power over individuals. Identification has been a critical tool for governments seeking to round up radicals or disfavored citizens.¹⁸³ It is also an efficient tool for controlling people. In the United States, passports were used to stifle dissent; since Communists during the McCarthy era were prohibited from using passports, they were restricted from traveling outside the country.¹⁸⁴

Identification can inhibit one's ability to be anonymous or pseudonymous.¹⁸⁵ Anonymity and pseudonymity protect people from bias based on their identities and enable people to vote, speak, and associate more freely by protecting them from the danger of reprisal.¹⁸⁶ Anonymity can enhance

¹⁸¹ SOLOVE, THE DIGITAL PERSON, *supra* note 40, at 1.

¹⁸² Clarke, *Information Systems*, *supra* note 169, at 20.

¹⁸³ As Richard Sobel observes, "[i]dentity systems and documents have a long history of uses and abuses for social control and discrimination." Richard Sobel, *The Degradation of Political Identity Under a National Identification System*, 8 B.U. J. SCI. & TECH. L. 37, 48 (2002). Indeed, one of the primary reasons that governments created passports and identity cards was to restrict movement, alter patterns of migration, and control the movements of poor people and others viewed as undesirable. Marc Garcelon, *Colonizing the Subject: The Genealogy and Legacy of the Soviet Internal Passport*, in DOCUMENTING INDIVIDUAL IDENTITY 83, 86 (Jane Caplan & John Torpey eds., 2001).

¹⁸⁴ Sobel, *supra* note 183, at 49.

¹⁸⁵ Anonymous speech has a long history as an important mode of expression. Between 1789 and 1809, numerous Presidents and Congressmen published anonymous political writings. SMITH, *supra* note 111, at 41. Ben Franklin used over forty pen names during his life. *Id.* at 43. Indeed, James Madison, Alexander Hamilton, and John Jay published the *Federalist Papers* using the pseudonym "Publius." *McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334, 343 n.6 (1995). The Anti-Federalists also used pseudonyms. *Id.*

¹⁸⁶ As Gary Marx notes, anonymity can "facilitate the flow of information and communication on public issues" and "encourage experimentation and risk taking without facing large consequences, risk of failure, or embarrassment since one's identity is protected." Gary

the persuasiveness of one's ideas, for identification can shade reception of ideas with readers' biases and prejudices. This is why, in many universities and schools, exams are graded anonymously. Anonymity provides people with the ability to criticize the companies they work for and to blow the whistle.¹⁸⁷ Anonymity also protects people who read or listen to certain unpopular ideas.¹⁸⁸

In a series of cases, the Supreme Court has recognized that "identification and fear of reprisal might deter perfectly peaceful discussions of public matters of importance."¹⁸⁹ Thus, requiring the disclosure of identifying information would chill free speech, violating the First Amendment. However, in *Hibel v. Sixth Judicial District Court*, the Court concluded that a law requiring people to identify themselves during a police stop did not violate the Fourth and Fifth Amendments.¹⁹⁰ In particular, responding to the Fifth Amendment challenge, the Court concluded: "Answering a request to disclose a name is likely to be so insignificant in the scheme of things as to be incriminating only in unusual circumstances."¹⁹¹ However, as Justice Stevens wrote in dissent:

A name can provide the key to a broad array of information about the person, particularly in the hands of a police officer with access to a range of law enforcement databases. And that information, in turn, can be tremendously useful in a criminal prosecution. It is therefore quite wrong to suggest that a person's identity provides a link in the chain to incriminating evidence "only in unusual circumstances."¹⁹²

T. Marx, *Identity and Anonymity: Some Conceptual Distinctions and Issues for Research*, in DOCUMENTING INDIVIDUAL IDENTITY, *supra* note 183, at 311, 316, 318 (2001); see also A. Michael Froomkin, *Flood Control on the Information Ocean: Living With Anonymity, Digital Cash, and Distributed Databases*, 15 J.L. & COM. 395, 408 (1996) ("Not everyone is so courageous as to wish to be known for everything they say, and some timorous speech deserves encouragement.").

¹⁸⁷ One of the most famous examples of an anonymous whistleblower is Deep Throat, Bob Woodward and Carl Bernstein's confidential source who helped them unearth the Watergate scandal. See CARL BERNSTEIN & BOB WOODWARD, *ALL THE PRESIDENT'S MEN* 71-73, 130-35 (1974).

¹⁸⁸ See Julie E. Cohen, *A Right to Read Anonymously: A Closer Look at "Copyright Management" in Cyberspace*, 28 CONN. L. REV. 981, 1012-14 (1996) (arguing that reader anonymity is an important First Amendment value and that anonymous reading protects people from being associated with the ideas about which they read).

¹⁸⁹ *Talley v. California*, 362 U.S. 60, 65 (1960); see also *Watchtower Bible & Tract Soc. v. Village of Stratton*, 536 U.S. 150, 166-67 (2002) (stating that anonymity protects people who engage in "unpopular causes"); *McIntyre*, 514 U.S. at 341-42 ("The decision in favor of anonymity may be motivated by fear of economic or official retaliation, by concern about social ostracism, or merely by a desire to preserve as much of one's privacy as possible.").

¹⁹⁰ 542 U.S. 177, 189, 190-91 (2004).

¹⁹¹ *Id.* at 191.

¹⁹² *Id.* at 196 (Stevens, J., dissenting) (quoting *id.* at 191 (majority opinion)).

Stevens's dissent recognizes that the harm of identification is often not in the disclosure of the identifying marker (the name, fingerprint, etc.) itself, but in the ability to connect this marker to a stream of collected data. Being asked to identify oneself, therefore, is being asked to link oneself to the data, not just state a name.

3. Insecurity

Identity theft is the fastest growing white collar crime.¹⁹³ An identity thief opens accounts and conducts fraud in the victim's name. As I have argued elsewhere, identity theft is made possible because we all have "digital dossiers"—extensive repositories of personal information about us—that are maintained by various companies and institutions.¹⁹⁴ The thief taps into a person's dossier, which becomes polluted with discrediting information when debts go unpaid, or when the thief uses the person's identity to commit a crime. Victims of identity theft are submerged into a bureaucratic hell where, according to one estimate, they must spend approximately two years and almost 200 hours to decontaminate their dossier.¹⁹⁵ While their dossier remains defiled, victims have difficulty getting jobs, loans, or mortgages.¹⁹⁶

Identity theft is the overt result of a larger group of problems I call "insecurity." Glitches, security lapses, abuses, and illicit uses of personal information all fall into this category. Insecurity, in short, is a problem caused by the way our information is handled and protected.

Insecurity is related to aggregation, as it creates risks of downstream harm that can emerge from inadequate protection of compendiums of personal data. Insecurity is also related to identification—it often occurs because of difficulties in linking data to people. As Lynn LoPucki observes, identity theft occurs because "creditors and credit-reporting agencies often lack both the means and the incentives to correctly identify the persons who seek credit from them or on whom they report."¹⁹⁷ In this sense, insecurity can be a cost of lack of identification.¹⁹⁸

¹⁹³ Jennifer 8. Lee, *Fighting Back When Someone Steals Your Name*, N.Y. TIMES, Apr. 8, 2001, § 3, at 8.

¹⁹⁴ SOLOVE, THE DIGITAL PERSON, *supra* note 40, at 110.

¹⁹⁵ JANINE BENNER ET AL., NOWHERE TO TURN: VICTIMS SPEAK OUT ON IDENTITY THEFT, pt. II, §§ 1, 4 (2000), <http://www.privacyrights.org/ar/idtheft2000.htm>.

¹⁹⁶ SOLOVE, THE DIGITAL PERSON, *supra* note 40, at 110.

¹⁹⁷ Lynn M. LoPucki, *Human Identification Theory and the Identity Theft Problem*, 80 TEX. L. REV. 89, 94 (2001).

¹⁹⁸ Identification via password, however, can enhance security without linking the individual up to immutable characteristics such as biometric identifiers.

Distortion—the dissemination of false information about a person—is related to insecurity, since problems with security can result in one's records being polluted with false data. This can destroy a person's financial reputation, which today is based in large part on the records maintained by credit reporting agencies.¹⁹⁹ Insecurity, therefore, can involve not only a threat of disclosure, but also a threat of distortion.

Insecurity exposes people to potential future harm. Combating identity theft after it happens has proven immensely difficult.²⁰⁰ The careless use of data by businesses and the government makes the crime of identity theft incredibly easy. Companies use Social Security numbers (SSNs) as passwords, and since SSNs can be readily obtained by identity thieves from public records or from database companies, people's accounts and personal information are insecure.²⁰¹

In cases involving the constitutional right to privacy, courts have sometimes recognized insecurity as a privacy harm. In *Whalen v. Roe*, the Supreme Court suggested that the constitutional right to privacy also extended to the "individual interest in avoiding disclosure of personal matters."²⁰² As the Court observed, the government's collection of personal data for its record systems "is typically accompanied by a concomitant statutory or regulatory duty to avoid unwarranted disclosures."²⁰³ The Court noted that "in some circumstances that duty arguably has its roots in the Constitution."²⁰⁴ Applying *Whalen*, a federal circuit court in *Fraternal Order of Police, Lodge No. 5 v. City of Philadelphia* concluded that certain questions on a police department employee questionnaire were unconstitutional because there were no guidelines about maintaining the security of the information.²⁰⁵

Many privacy statutes require that information be kept secure. This requirement was proposed in the original Fair Information Practices of 1973: "Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take reasonable precautions to prevent misuse of the

¹⁹⁹ See NOCK, *supra* note 148, at 53 (recounting the rise of credit bureaus). For a comprehensive account of the credit reporting system, see EVAN HENDRICKS, CREDIT SCORES & CREDIT REPORTS (2004).

²⁰⁰ See SOLOVE, THE DIGITAL PERSON, *supra* note 40, at 111-12 (noting that investigation and prosecution of identity theft cases is not a top priority for law enforcement agencies, and that victims are slow to realize that their identity has been stolen).

²⁰¹ *Id.* at 115-19.

²⁰² 429 U.S. 589, 599 (1977).

²⁰³ *Id.* at 605.

²⁰⁴ *Id.*

²⁰⁵ 812 F.2d 105, 118 (3d Cir. 1987).

data.”²⁰⁶ The Privacy Act of 1974 requires federal agencies maintaining personal data to “establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records.”²⁰⁷ The Children’s Online Privacy Protection Act states that websites must protect the “confidentiality, security, and integrity of personal information collected from children.”²⁰⁸ The Gramm-Leach-Bliley Act requires that regulatory agencies of financial institutions establish security standards for personal information.²⁰⁹ The Health Insurance Portability and Accountability Act of 1996 requires the promulgation of security standards “to ensure the integrity and confidentiality of [medical] information.”²¹⁰ The Computer Fraud and Abuse Act prohibits hacking into people’s computers.²¹¹

Although the law recognizes injuries when a breach in security results in overt harm to an individual, courts are reluctant to find harm simply from the insecure storage of information.²¹² Several privacy statutes attempt to avoid problems in measuring harm by providing for minimum liquidated damages.²¹³ In many instances, courts ignore insecurity as a problem. For example, in *Board of Education v. Earls*, a school district in Tecumseh, Oklahoma adopted a drug testing policy that required all middle and high school students to undergo drug testing before participating in any extracurricular activity.²¹⁴ Some of the students challenged the policy under the Fourth Amendment, but the Supreme Court upheld the testing.²¹⁵ The students contended that the school was careless in protecting the security of the

²⁰⁶ U.S. DEP’T OF HEALTH, EDUC., & WELFARE, *supra* note 168, at 41.

²⁰⁷ 5 U.S.C. § 552a(e)(10) (2000).

²⁰⁸ 15 U.S.C. § 6502(b)(1)(D) (2000).

²⁰⁹ 15 U.S.C. §§ 6801(b), 6805(b)(2) (2000). For the FTC’s security regulations, see 16 C.F.R. § 314 (2005).

²¹⁰ 42 U.S.C. § 1320d-2(d)(2) (2000).

²¹¹ 18 U.S.C. § 1030 (2000 & Supp. 2002).

²¹² See Daniel J. Solove, *The New Vulnerability: Data Security and Personal Information*, in *SECURING PRIVACY IN THE INTERNET AGE* 11-12 (Margaret Jane Radin et al. eds., forthcoming 2006), available at <http://ssrn.com/abstract=583483> (arguing that the law fails to adequately guard sensitive information, and that a reconceptualization of the legal duties information-keepers owe their customers is necessary).

²¹³ See, e.g., Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2707(c) (2000) (setting a minimum \$1000 fine per violation); Video Privacy Protection Act of 1988, 18 U.S.C. § 2710(c) (2000) (setting liquidated damages of \$2500 as the minimum amount recoverable from a defendant found to have wrongfully disclosed video tape rental or sale records). The Privacy Act of 1974 also contains a liquidated damages provision; however, the Supreme Court interpreted it to apply only when the plaintiff demonstrates actual damages. See *Doe v. Chao*, 540 U.S. 614, 616 (2004) (construing 5 U.S.C. § 552a(g)(4) (2000)).

²¹⁴ 536 U.S. 822, 826 (2002).

²¹⁵ *Id.* at 827, 838.

test results.²¹⁶ Files were not carefully secured and were left where they could be accessed by unauthorized people, such as other students.²¹⁷ The Court dismissed this contention because there were no allegations of any improper disclosures.²¹⁸ What the court failed to recognize is that disclosure differs from insecurity because the harm caused by disclosure is the actual leakage of information; insecurity is the injury of being placed in a weakened state, of being made more vulnerable to a range of future harms. Although insecurity increases the possibility of disclosure, courts will often not recognize a harm unless there has been actual disclosure.

4. Secondary Use

In 1977, in an attempt to capture people engaged in fraud, the federal government began matching its employee records with the records of individuals receiving federal benefits.²¹⁹ Some of these government matching programs used information obtained from businesses to uncover fraud.²²⁰ These matchings were done electronically through the use of computers, and they led to the investigations of millions of people.²²¹ In 1988, Congress passed the Computer Matching and Privacy Protection Act to regulate computer matching.²²² *Should lead*

In 1973, the U.S. Department of Health, Education, and Welfare (HEW) in its influential report on the harms caused by computer databases, set forth a series of Fair Information Practices, one of which provides that "[t]here must be a way for an individual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent."²²³ This principle, which has become known as the purpose specification principle, has been embodied in various privacy

²¹⁶ *Id.* at 833.

²¹⁷ *Id.* at 848 (Ginsburg, J., dissenting).

²¹⁸ See *id.* at 833 (majority opinion) (asserting that because there was no report of a student actually viewing another student's medical record, the carelessness alleged did not rise to the level of a privacy intrusion).

²¹⁹ REGAN, *supra* note 43, at 86; Robert Gellman, *Does Privacy Law Work?*, in TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE 193, 198-99 (Philip E. Agre & Marc Rotenberg eds., 1997).

²²⁰ See GARY T. MARX, UNDERCOVER: POLICE SURVEILLANCE IN AMERICA 209-10 (1988) (citing instances of government agencies—including the Selective Service and the IRS—using databases supplied by private businesses to investigate instances of draft-dodging and tax fraud).

²²¹ *Id.* at 208-11.

²²² Computer Matching and Privacy Protection Act (CMPPA) of 1988, Pub. L. No. 100-503, 102 Stat. 2507 (codified at 5 U.S.C. § 552a (2000)).

²²³ U.S. DEP'T OF HEALTH, EDUC., & WELFARE, *supra* note 168, at 41-42 (1973).

principles and laws. The Privacy Act of 1974, for example, requires agencies to inform people of "the principal purpose or purposes for which the information is intended to be used" when their information is collected.²²⁴ The Fair Credit Reporting Act of 1970 limits the purposes for which credit reports can be used.²²⁵ The Driver's Privacy Protection Act of 1994 makes it "unlawful for any person knowingly to obtain or disclose personal information, from a motor vehicle record, for any use not permitted [by the Act]."²²⁶ Anybody who uses an individual's personal data obtained from a motor vehicle record for an impermissible purpose is subject to civil liability.²²⁷ The Cable Communications Policy Act of 1984 requires cable operators to "destroy personally identifiable information if the information is no longer necessary for the purpose for which it was collected."²²⁸ The Gramm-Leach-Bliley Act of 1999 places limits on the "reuse" of personal data when a company provides it to another company.²²⁹ The Video Privacy Protection Act of 1988 has a similar provision for personal information collected about video rental customers.²³⁰ The Federal Election Campaign Act states that records of contributors to political committees are "available for public inspection . . . except that any information copied from such reports . . . may not be sold or used by any person for the purpose of soliciting contributions or for commercial purposes."²³¹ The Health Insurance Portability and Accountability Act regulations restrict secondary uses of medical information beyond those necessary for treatment, payment, and health care operations.²³²

very specific

What is the concern over secondary uses of information beyond those purposes for which it is collected? Why are there so many legal attempts to limit secondary uses of data?

"Secondary use" is the use of data for purposes unrelated to the purposes for which the data was initially collected without the data subject's consent. There are certainly many desirable instances of secondary use. Information might be used to stop a crime or to save a life. The variety of possible secondary uses of data is virtually infinite, and they range from benign to malignant.

²²⁴ 5 U.S.C. § 552a(e)(3)(B) (2000).

²²⁵ 15 U.S.C. § 1681b (2000 & Supp. 2002).

²²⁶ 18 U.S.C. § 2722(a) (2000).

²²⁷ 18 U.S.C. § 2722 (2000).

²²⁸ 47 U.S.C. § 551(e) (2000).

²²⁹ 15 U.S.C. § 6802(c) (2000).

²³⁰ 18 U.S.C. § 2710(e) (2000).

²³¹ 2 U.S.C. § 438(a)(4) (2000).

²³² 45 C.F.R. § 164.508(a) (2000).

Secondary use can cause problems. It creates a dignitary harm, as it involves using information in ways to which a person does not consent and might not find desirable. Secondary uses thwart people's expectations about how the data they give out will be used. People might not give out data if they know about a potential secondary use, such as for telemarketing, spam, or other forms of intrusive advertising. Fingerprints of United States military recruits originally collected to screen their backgrounds were sent to the FBI and incorporated into the FBI's criminal fingerprint database.²³³ Such individuals may not have expected nor desired to have their fingerprints maintained in a law enforcement database of convicts and criminals. Secondary use resembles breach of confidentiality, in that there is a betrayal of the person's expectations when giving out information.

One argument to the contrary is that people should simply expect that their data might be used in different ways when they relinquish it. Under this theory, there is no harm to expectations. But even with privacy policies stating that information might be used in secondary ways, people often do not read or understand these policies. Nor can they appropriately make an informed decision about secondary uses since they might have little idea about the range of potential uses. According to Paul Schwartz, this is an asymmetry of knowledge problem:

[I]ndividuals are likely to know little or nothing about the circumstances under which their personal data are captured, sold, or processed. This widespread individual ignorance hinders development through the privacy marketplace of appropriate norms about personal data use. The result of this asymmetrical knowledge will be one-sided bargains that benefit data processors.²³⁴

The potential for secondary use generates fear and uncertainty over how one's information will be used in the future, creating a sense of powerlessness and vulnerability. In this respect, secondary use resembles the harm created by insecurity. The harm is a dignitary one, emerging from denying people control over the future use of their data, which can be used in ways that have significant effects on their lives.

Secondary use also creates architectural problems. The secondary use of information can create problems because the information may not fit as well with the new use. When removed from the original context in which it was collected, data can more readily be misunderstood.

²³³ Pamela Sankar, *DNA-Typing: Galton's Eugenic Dream Realized?*, in DOCUMENTING INDIVIDUAL IDENTITY, *supra* note 183, at 273, 278-79.

²³⁴ Schwartz, *supra* note 18, at 1683.

What are expectations

5. Exclusion

Among the Fair Information Practices are three related principles: (1) the existence of record systems cannot be kept secret; (2) an individual must be able to "find out what information about him is in a record and how it is used"; and (3) an individual must be able to "correct or amend a record of identifiable information about him."²³⁵ Together these principles aim to allow individuals to have some knowledge of and input into the records about them maintained by government agencies and businesses. The principles require transparency in the record systems and provide individuals with a right to ensure that the information is accurate. What problems or harms are caused when people are not informed about the information entities have about them?

I refer to the failure to provide individuals with notice and input about their records as *exclusion*. There are a number of justifications for exclusion. Providing notice to people about the uses of their personal information and giving them rights to access and correct it can be costly. Also, government agencies might want to keep certain record systems pertaining to law enforcement or intelligence confidential so as not to tip off those who are being investigated.

Exclusion, however, creates an architectural problem. Exclusion reduces accountability on the part of government agencies and businesses that maintain records about individuals. Exclusion is also related to insecurity, as the lack of accountability often goes hand-in-hand with inadequate security in record systems of personal data. Exclusion is different than insecurity in that exclusion is not primarily a harm caused by the lack of protection against data leakage or contamination. Rather, it is a harm created by being shut out from participating in the use of one's personal data, by not being informed about how that data is used, and by not being able to do anything to affect how it is used.

One might contend that exclusion is not a harm in and of itself but is merely a factor that leads to downstream harms like information dissemination. Exclusion, however, can be harmful even if it does not lead to the dissemination of data. As with secondary use and insecurity, exclusion creates a sense of vulnerability and uncertainty in individuals. An inability to participate in the maintenance and use of one's information can lead to feelings of powerlessness and frustration. Some might argue that there are many aspects of life in which we are powerless, and that there is nothing special about powerlessness with respect to personal information. But in a world

²³⁵ U.S. DEP'T OF HEALTH, EDUC., & WELFARE, *supra* note 168, at 41.

where personal information is increasingly used to make important decisions about our lives, powerlessness in this arena can be significantly troublesome.

Tort law, by and large, has not recognized exclusion as a harm. In certain kinds of special relationships, however, tort law has developed strong duties and responsibilities. The law of fiduciary duties creates special duties of accountability within certain relationships. A fiduciary relationship exists when one party stands in a special position of power over another person.²³⁶ New York Chief Justice Benjamin Cardozo described the relationship best when he wrote:

Many forms of conduct permissible in a workaday world for those acting at arm's length, are forbidden to those bound by fiduciary ties. A trustee is held to something stricter than the morals of the market place. Not honesty alone, but the punctilio of an honor the most sensitive, is then the standard of behavior.²³⁷

Fiduciary relationships have been held to protect privacy in certain relationships.²³⁸ In this way, exclusion is related to the harm of breach of confidentiality, which is discussed later in this taxonomy.²³⁹ Moreover, in certain relationships, such as between doctors and patients, fiduciary duties require informed consent. As one court has noted, "in soliciting the patient's consent, a physician has a fiduciary duty to disclose all information material to the patient's decision."²⁴⁰ Therefore, tort law has at least recognized the concept of accountability, although courts have not recognized the maintenance of personal information about a person as giving rise to fiduciary obligations. Such a development is not foreclosed, however, as courts

but not
data

²³⁶ See *Mobil Oil Corp. v. Rubenfeld*, 339 N.Y.S.2d 623, 632 (Civ. Ct. 1972) (defining a fiduciary relationship as one "founded on trust or confidence").

²³⁷ *Meinhard v. Salmon*, 164 N.E. 545, 546 (N.Y. 1928).

²³⁸ For example, the tort of breach of confidentiality protects the privacy of people's communications with their doctors, bankers, lawyers, and others. See *Ind. Nat'l Bank v. Chapman*, 482 N.E.2d 474, 482 (Ind. Ct. App. 1985) (holding that a bank has a duty not to disclose customer information unless it is to someone with a legitimate public interest); *Kohn v. Schiappa*, 656 A.2d 1322, 1323 (N.J. Super. Ct. Law Div. 1995) (allowing a claim of negligence where an attorney harmed a client by disclosing confidential information); *Biddle v. Warren Gen. Hosp.*, 715 N.E.2d 518, 523 (Ohio 1999) (recognizing a cause of action when physicians breach confidentiality); *McCormick v. England*, 494 S.E.2d 431, 435 (S.C. Ct. App. 1997) (same). Jessica Litman proposes that the breach of confidentiality tort apply to companies that trade in personal information. Jessica Litman, *Information Privacy/Information Property*, 52 STAN. L. REV. 1283, 1304-13 (2000).

²³⁹ See *infra* Part C.1.

²⁴⁰ *Moore v. Regents of the Univ. of Cal.*, 793 P.2d 479, 483 (Cal. 1990) (en banc).

"have carefully refrained from defining instances of fiduciary relations in such a manner that other and perhaps new cases might be excluded."²⁴¹

The primary legal protection against exclusion is statutory. Federal privacy statutes guard against exclusion by mandating transparency and granting individuals the right to access their information. For example, the Privacy Act provides people the right to access their records.²⁴² So do the Cable Communications Policy Act,²⁴³ the Fair Credit Reporting Act,²⁴⁴ and the Children's Online Privacy Protection Act.²⁴⁵ Several privacy statutes allow people a mechanism to demand the correction of inaccurate information in their records.²⁴⁶ While these statutes stop short of requiring informed consent, they do give people some ability to discover the information gathered about them.

Some statutes also allow people to opt out of certain uses of information. The Gramm-Leach-Bliley Act, for example, allows people to refuse to allow financial institutions to share their data with third parties.²⁴⁷ The opt-out right, which assumes consent unless an individual affirmatively indicates a preference for not sharing the information, does not ensure that consent is informed beyond providing customers with notice that information may be shared. Accordingly, it would most likely fail to constitute informed consent within a fiduciary relationship.

C. Information Dissemination

Thus far, I have discussed harms arising out of the collection of information as well as harms arising from the storage and use of data. "Information dissemination" is one of the broadest groupings of privacy harms. These harms consist of the revelation of personal data or the threat of spreading information. This group includes (1) breach of confidentiality, (2) disclosure, (3) exposure, (4) increased accessibility, (5) blackmail, (6) appropriation, and (7) distortion.

²⁴¹ *Swerhun v. Gen. Motors Corp.*, 812 F. Supp. 1218, 1222 (M.D. Fla. 1993) (quoting *Quinn v. Phipps*, 113 So. 419, 421 (Fla. 1927)).

²⁴² 5 U.S.C. § 552a(d) (2000).

²⁴³ 47 U.S.C. § 551(d) (2000).

²⁴⁴ 15 U.S.C. § 1681g(a) (2000).

²⁴⁵ *Id.* § 6502(b)(1)(B)(i).

²⁴⁶ *See, e.g.*, Fair Credit Reporting Act, *id.* § 1681i(a)(5)(A).

²⁴⁷ *See id.* § 6802(b).

1. Breach of Confidentiality

Mrs. McCormick was involved in a contentious divorce and custody battle with her husband. McCormick's doctor gave a letter to her husband that stated that McCormick was suffering from "major depression and alcoholism, acute and chronic."²⁴⁸ McCormick sued her doctor. According to the court, a "majority of the jurisdictions faced with the issue have recognized a cause of action against a physician for the unauthorized disclosure of confidential information unless the disclosure is compelled by law or is in the patient's interest or the public interest."²⁴⁹ Unlike the tort of public disclosure, the tort of breach of confidentiality does not require that the disclosure be "highly offensive."²⁵⁰ The court reasoned that the public disclosure tort "focuses on the content, rather than the source of the information. The unauthorized revelation of confidential medical information should be protected without regard to the degree of its offensiveness."²⁵¹ The tort of breach of confidentiality applies not only to physicians, but also to bankers and other professionals who maintain relationships of trust.²⁵² Additionally, some courts have extended liability to third parties who induce the physician to disclose.²⁵³

Why does the law recognize a separate cause of action for breach of confidentiality? Why not rectify such harms with the tort of public disclosure?

The answer, I posit, is that disclosure and breach of confidentiality cause different kinds of injuries. Both involve the revelation of secrets about a person, but breaches of confidentiality also violate the trust in a specific relationship. In this way, the tort emerges from the concept of a fidu-

So what?

²⁴⁸ McCormick v. England, 494 S.E.2d 431, 432 (S.C. Ct. App. 1997).

²⁴⁹ *Id.* at 435 (citations omitted).

²⁵⁰ *Id.* at 438.

²⁵¹ *Id.*

²⁵² See, e.g., Peterson v. Idaho First Nat'l Bank, 367 P.2d 284, 290 (Idaho 1961) (recognizing a breach of confidentiality tort for disclosure by a bank). For more information on the breach of confidentiality tort, see generally Alan B. Vickery, Note, *Breach of Confidence: An Emerging Tort*, 82 COLUM. L. REV. 1426, 1426 (1982) (identifying "the present contours of the . . . tort" and proposing a general rule for its application). Interestingly, England, which does not recognize the privacy torts, does recognize breach of confidence, which has become the country's central means of protecting privacy. RAYMOND WACKS, *PRIVACY AND PRESS FREEDOM* 48-58 (1995). Unlike the American version, which applies only in a few narrow contexts (mainly to the patient-physician relationship), the English tort applies much more generally and extends even to spouses and lovers. *Id.* at 51.

²⁵³ See *Hammonds v. Aetna Cas. & Sur. Co.*, 243 F. Supp. 793 (N.D. Ohio 1965) (holding an insurance company liable for inducing a physician to disclose confidential information).

ciary relationship, which is "founded on trust or confidence reposed by one person in the integrity and fidelity of another."²⁵⁴

The harm from a breach of confidence, then, is not simply that information has been disclosed, but that the victim has been betrayed. When it recognized a cause of action for breach of confidentiality in 1920, the court in *Simonsen v. Swenson* noted that "the physician is bound, . . . upon his own professional honor and the ethics of his high profession, to keep secret [a patient's information]. . . . A wrongful breach of such confidence, and a betrayal of such trust, would give rise to a civil action for the damages naturally flowing from such wrong."²⁵⁵

Protection against breach of confidentiality helps promote certain relationships that depend upon trust. The disclosure tort also protects relationships of trust, but disclosure must result in the release of embarrassing secrets or discrediting data before courts will consider it to be harmful.²⁵⁶ Breach of confidentiality requires only a betrayal of trust, regardless of the nature of the data revealed.

There are certainly instances where we might find the breach of confidentiality desirable. In *Simonsen*, for example, the court concluded that a doctor should not be held liable for disclosing the fact that a patient had syphilis, which at the time was believed to be a highly contagious disease.²⁵⁷ The court held that protecting public health outweighed any privacy interest the plaintiff might have.²⁵⁸ Likewise, in *Tarasoff v. Regents of the University of California*, a psychotherapy patient murdered a young woman with whom he was obsessed.²⁵⁹ The court concluded that the patient's psychotherapist had a duty to the woman because he had knowledge that his patient posed a danger to her:

[T]he therapist's obligations to his patient require that he not disclose a confidence unless such disclosure is necessary to avert danger to others, and even then that he do so discreetly, and in a fashion that would preserve the privacy of his patient to the fullest extent compatible with the prevention of the threatened danger.²⁶⁰

The law, however, is inconsistent in its recognition of breach of confidentiality as a harm. Fourth Amendment law fails altogether to recognize the breach of confidentiality as a harm. In *United States v. Miller*, federal

before highly
sensitive

²⁵⁴ *Mobil Oil Corp. v. Rubinfeld*, 339 N.Y.S.2d 623, 632 (Civ. Ct. 1972).

²⁵⁵ 177 N.W. 831, 832 (Neb. 1920).

²⁵⁶ See *infra* notes 289-93 and accompanying text.

²⁵⁷ 177 N.W. at 831.

²⁵⁸ *Id.* at 832.

²⁵⁹ 551 P.2d 334, 339-40 (Cal. 1976) (en banc).

²⁶⁰ *Id.* at 347.

law enforcement officials issued subpoenas to two banks to produce a customer's financial records.²⁶¹ The banks complied with the subpoenas, but the customer was not notified of the disclosure of the records until later in the course of prosecution.²⁶² The defendant contended that the subpoenas violated his Fourth Amendment rights.²⁶³ The Court concluded, however, that the customer lacked a reasonable expectation of privacy in the financial records maintained by his bank.²⁶⁴ According to the Court, "the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities."²⁶⁵ Moreover, the Court contended, "[a]ll of the documents obtained, including financial statements and deposit slips, contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business."²⁶⁶

3d party

A few years later, the Court employed similar reasoning in *Smith v. Maryland*, where it held that people lack a reasonable expectation of privacy in the phone numbers they dial because people "know that they must convey numerical information to the phone company" and, therefore, they cannot "harbor any general expectation that the numbers they dial will remain secret."²⁶⁷

Miller and *Smith* are the leading cases in what has become known as the "third party doctrine."²⁶⁸ This doctrine provides that if information is possessed or known by third parties, then, for purposes of the Fourth Amendment, an individual lacks a reasonable expectation of privacy in the information. In the Information Age, much of what we do is recorded by third parties.²⁶⁹ The third party doctrine therefore places an extensive amount of personal information outside the protection of the Fourth Amendment.²⁷⁰

The third party doctrine is based on the secrecy paradigm: since others know the information, it is no longer completely secret. But the fact that the information is known to third parties would not be relevant to the Court's analysis if the harm were understood to be a breach of confidentiality.

²⁶¹ 425 U.S. 435, 437 (1976) (limited by Right to Financial Privacy Act of 1978, 12 U.S.C. §§ 3401-3421 (2000)).

²⁶² *Id.* at 438.

²⁶³ *Id.* at 438-39.

²⁶⁴ *Id.* at 442.

²⁶⁵ *Id.* at 443.

²⁶⁶ *Id.* at 442.

²⁶⁷ 442 U.S. 735, 743 (1979).

²⁶⁸ SOLOVE, THE DIGITAL PERSON, *supra* note 40, at 201.

²⁶⁹ See *id.* at 202-09 (discussing the consequences of applying outdated privacy protection schemes to modern times).

²⁷⁰ *Id.* at 201-02.

When people establish a relationship with banks, Internet service providers, phone companies, and other businesses, they are not disclosing their information to the world. They are giving it to a party with implicit (and often explicit) promises that the information will not be disseminated.²⁷¹

Unlike Fourth Amendment law, tort law recognizes breach of confidentiality as a distinct harm. The breach of confidentiality tort applies to the patient-physician relationship and to other relationships as well. As mentioned previously, some courts have held that the tort applies to banks.²⁷² In *Peterson v. Idaho First National Bank*, the court observed: "All agree that a bank should protect its business records from the prying eyes of the public, moved by curiosity or malice. No one questions its right to protect its fiduciary relationship with its customers, which, in sound banking practice, as a matter of common knowledge, is done everywhere."²⁷³ Not divulging customers' financial information to others "is an implied term of the contract between a banker and his customer."²⁷⁴ Moreover, the court reasoned: "In-violate secrecy is one of the inherent and fundamental precepts of the relationship of the bank and its customers or depositors."²⁷⁵ Many other courts have agreed.²⁷⁶

yes

2. Disclosure

The law has developed a number of protections against disclosures of true information about people. The tort of public disclosure of private facts, inspired by Warren and Brandeis's article, creates a cause of action for one who publicly discloses a private matter that is "highly offensive to a reason-

²⁷¹ See, e.g., *Brex v. Smith*, 146 A. 34, 36 (N.J. Ch. 1929) (finding an "implied obligation" on banks to keep customers' bank records confidential until compelled by a court to disclose them).

²⁷² See *supra* note 252 and accompanying text.

²⁷³ 367 P.2d 284, 290 (Idaho 1961) (quoting *United States v. First Nat'l Bank of Mobile*, 67 F. Supp. 616, 624 (S.D. Ala. 1946)).

²⁷⁴ *Id.* at 290 (quoting 7 AM. JUR. *Banks* § 196 (1937)).

²⁷⁵ *Id.*

²⁷⁶ See, e.g., *Barnett Bank of W. Fla. v. Hooper*, 498 So. 2d 923, 926 (Fla. 1986) (recognizing that banks establish fiduciary relationships with customers when they enter into transactions); *Ind. Nat'l Bank v. Chapman*, 482 N.E.2d 474, 482 (Ind. Ct. App. 1985) (finding an implied contract not to disclose personal financial information between a bank and its customers); *Suburban Trust Co. v. Waller*, 408 A.2d 758, 762 (Md. Ct. Spec. App. 1979) ("[A] bank implicitly warrants to maintain, in strict confidence, information regarding its depositor's affairs."); *Richfield Bank & Trust Co. v. Sjogren*, 244 N.W.2d 648, 651 (Minn. 1976) (recognizing a duty of confidentiality for banks); *McGuire v. Shubert*, 722 A.2d 1087, 1091 (Pa. Super. Ct. 1998) (finding a duty for a bank to keep its customers' account information confidential).

able person" and "is not of legitimate concern to the public."²⁷⁷ In *Whalen v. Roe*, the Supreme Court recognized that the "right to privacy" based on substantive due process also encompassed the "individual interest in avoiding disclosure of personal matters."²⁷⁸ Although this branch of the right to privacy has not received much further elaboration by the Court, it is recognized in many circuits, where it can enable plaintiffs to sue government officials for disclosing personal information.²⁷⁹ Further, a number of statutes restrict disclosure of information from government records,²⁸⁰ school records,²⁸¹ cable company records,²⁸² video records,²⁸³ motor vehicle records,²⁸⁴ and health records.²⁸⁵ Various states have restricted the disclosure of particular forms of information, such as ~~medical data and alcohol and drug abuse.~~²⁸⁶

Why does the law protect people against the disclosure of true information about them? Some critics of such protections contend that they infringe upon free speech. Eugene Volokh argues that "the right to information privacy—my right to control your communication of personally identifiable information about me—is a right to have the government stop you from speaking about me."²⁸⁷ Others have charged that protection against disclo-

²⁷⁷ RESTATEMENT (SECOND) OF TORTS § 652D (1977); see Warren & Brandeis, *supra* note 21, at 195-96.

²⁷⁸ 429 U.S. 589, 598-99 (1977).

²⁷⁹ See, e.g., *Doe v. Borough of Barrington*, 729 F. Supp. 376, 382 (D.N.J. 1990) (holding that it was a violation of the plaintiff's constitutional right to information privacy for police to disclose to neighbors that the plaintiff's husband was infected with AIDS).

²⁸⁰ See Privacy Act of 1974, 5 U.S.C. § 552a(c)(10) (2000) (prohibiting agencies from disclosing information about an individual without her prior written consent).

²⁸¹ See Family Educational Rights and Privacy Act of 1974, 20 U.S.C. § 1232g(b)(1) (2000) (requiring educational agencies or institutions that receive government funding not to disclose education records without written consent).

²⁸² See Cable Communications Policy Act of 1984, 47 U.S.C. §§ 551(b)-(c) (2000) (limiting the extent to which a cable service may collect or disclose personally identifiable information about subscribers).

²⁸³ See Video Privacy Protection Act of 1988, 18 U.S.C. § 2710(b)(1) (2000) (creating civil liability for video stores that disclose personally identifiable information about any customer).

²⁸⁴ See Driver's Privacy Protection Act of 1994, 18 U.S.C. §§ 2721-2725 (2000) (restricting the use of personal information contained in state motor vehicle records).

²⁸⁵ See Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. § 1320d-2 (2000) (protecting the privacy of personal health information in transactions).

²⁸⁶ See, e.g., CAL. HEALTH & SAFETY CODE § 199.21 (West 1990) (repealed 1995) (prohibiting, inter alia, disclosure of HIV test results); N.Y. PUB. HEALTH LAW § 17 (McKinney 2001) (permitting the release of medical records of minors relating to sexually transmitted diseases and abortion upon written request, but prohibiting the disclosure to parents without consent); 71 PA. STAT. ANN. § 1690.108 (West 1990) (prohibiting the disclosure of all records prepared during alcohol or drug abuse treatment).

²⁸⁷ Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right To Stop People from Speaking About You*, 52 STAN. L. REV. 1049, 1050-51

sure inhibits our ability to judge others and determine whether they are worthy of our trust. According to Richard Posner, disclosure protections provide people the "power to conceal information about themselves that others might use to their disadvantage."²⁸⁸

"Disclosure" occurs when certain true information about a person is revealed to others. Disclosure differs from breach of confidentiality because the harm in disclosure involves the damage to reputation caused by the dissemination; the harm with breach of confidentiality is the violation of trust in the relationship.²⁸⁹ Disclosure can harm even if the information is revealed by a stranger. In *The Right to Privacy*, Warren and Brandeis took issue with the argument that express or implied contractual duties of confidentiality could adequately protect privacy.²⁹⁰ In particular, they noted that strangers were increasingly able to gather personal information:

The narrower doctrine [of breach of contract] may have satisfied the demands of society at a time when the abuse to be guarded against could rarely have arisen without violating a contract or a special confidence; but now that modern devices afford abundant opportunities for the perpetration of such wrongs without any participation by the injured party, the protection granted by the law must be placed upon a broader foundation.²⁹¹

Warren and Brandeis pointed to new technologies of photography. Previously, cameras were large and expensive, and people had to sit and pose for their picture to be taken. This gave rise to a relationship with implicit contractual terms. But the invention of the "snap camera," a smaller camera that could take candid photographs, "rendered it possible to take pictures surreptitiously."²⁹² This led Warren and Brandeis to conclude that "the doctrines of contract and of trust are inadequate to support the required protection."²⁹³

Although protecting against disclosure does limit freedom of speech, disclosure can inhibit the very interests free speech protects. Protection from disclosure, like free speech, promotes individual autonomy. The risk of disclosure can prevent people from engaging in activities that further

tech change

(2000); see also THOMAS I. EMERSON, *THE SYSTEM OF FREEDOM OF EXPRESSION* 556 (1970) ("[T]he right of privacy depends upon guaranteeing an individual freedom from intrusion and freedom to think and believe, not freedom from discussion of his opinions, actions or affairs.").

²⁸⁸ RICHARD A. POSNER, *THE ECONOMICS OF JUSTICE* 271 (1983).

²⁸⁹ See *supra* Part C.1.

²⁹⁰ Warren & Brandeis, *supra* note 21, at 210.

²⁹¹ *Id.* at 210-11.

²⁹² *Id.* at 211.

²⁹³ *Id.*

their own self-development.²⁹⁴ Second, as with free speech, disclosure protections further democratic self-governance. A substantial amount of political discourse does not occur on public soap boxes, but rather in private conversations.²⁹⁵ Disclosure can inhibit people from associating with others, impinging upon freedom of association, and can also destroy anonymity, which is sometimes critical for the promotion of free expression.²⁹⁶

Disclosure can also threaten people's security. For example, many people have good reason to keep their addresses secret, including victims of stalking and domestic abuse attempting to hide from those that threaten them, police officers and prosecutors fearing retaliation by criminals, celebrities desiring to avoid harassment by paparazzi, and doctors who perform abortions desiring to protect their family's safety. People want to protect information that makes them vulnerable or that can be used by others to harm them physically, emotionally, financially, and reputationally. For example, in *Remsburg v. Docusearch, Inc.*, a deranged man was obsessed with Amy Lynn Boyer.²⁹⁷ He purchased Boyer's Social Security number and employment address from a database company called Docusearch. The man went to Boyer's workplace and murdered her. The court concluded that "threats posed by stalking and identity theft lead us to conclude that the risk of criminal misconduct is sufficiently foreseeable so that an investigator has a duty to exercise reasonable care in disclosing a third person's personal information to a client."²⁹⁸

In many instances, disclosure of information about a person will not enhance our ability to judge her; in fact, it can distort our assessments.²⁹⁹ Knowing bits and pieces of gossip about a person will often not paint a more complete portrait; it can lead to misimpressions and condemnation without full understanding. Disclosure protections also guard against irra-

²⁹⁴ See Daniel J. Solove, *The Virtues of Knowing Less: Justifying Privacy Protections Against Disclosure*, 53 DUKE L.J. 967, 990-92 (2003) [hereinafter Solove, *Virtues*].

²⁹⁵ *Id.* at 994.

²⁹⁶ See *id.* at 995 ("Protection against disclosure protects freedom of association, for it enables people to join together and exchange information without having to fear loss of employment, community shunning, and other social reprisals." (footnote omitted)).

²⁹⁷ 816 A.2d 1001, 1005-06 (N.H. 2003).

²⁹⁸ *Id.* at 1008.

²⁹⁹ See JEFFREY ROSEN, *THE UNWANTED GAZE: THE DESTRUCTION OF PRIVACY IN AMERICA 200* (2000) ("[C]hanges in media technology have increased the risk of mistaking information for knowledge."); Lawrence Lessig, *Privacy and Attention Span*, 89 GEO. L.J. 2063, 2068-69 (2001) (arguing that access to limited amounts of information only "creates the impression of knowledge"); Solove, *Virtues*, *supra* note 294, at 1037 ("Much misunderstanding occurs because of the disclosure of private information . . .").

tional judgment based on stereotypes of misinformation about diseases.³⁰⁰ Likewise, society may want to inhibit certain rational judgments, such as employment decisions based on genetic information. Even if employers are correct that a prospective employee with a genetic risk for developing a certain condition is, on balance, riskier to hire than a prospective employee without such a predisposition, even such a rational discriminatory employment decision has its costs. Such decisions may penalize people for things they cannot control and deter people from learning their genetic makeup.³⁰¹

Disclosure can also be harmful because it makes a person a "prisoner of [her] recorded past."³⁰² People grow and change, and disclosures of information from their past can inhibit their ability to reform their behavior, to have a second chance, or to alter their life's direction. Moreover, when information is released publicly, it can be used in a host of unforeseeable ways, creating problems related to those caused by secondary use.

The law often protects against disclosure when the information is kept secret but not when others know about it. As one court observed, appearing in public "necessarily involves doffing the cloak of privacy which the law protects."³⁰³ In *Penwell v. Taft Broadcasting Co.*, the court held that a husband and wife wrongfully arrested in public had no privacy interest against the broadcast of video footage of the arrest because it was filmed in public and was "left open to the public eye."³⁰⁴ Moreover, if a fact about a person is known to others, many courts conclude that it is no longer private. This was the case in *Sipple v. Chronicle Publishing Co.*, where newspapers "outed" Oliver Sipple, who heroically saved President Ford from an assassination attempt.³⁰⁵ The court concluded that his sexuality was not private because it was well known in the gay community.³⁰⁶ In *Duran v. Detroit News, Inc.*, a former Colombian judge was attempting to lay low because of death threats and a bounty placed on her head by a drug lord.³⁰⁷ When a newspaper disclosed her address, a court found no privacy interest because

³⁰⁰ See Solove, *Virtues*, *supra* note 294, at 1041-42 (describing the stigma attached to those with certain diseases and illnesses).

³⁰¹ *Cf. id.* at 1042-43.

³⁰² U.S. DEP'T OF HEALTH, EDUC., & WELFARE, *supra* note 168, at 112.

³⁰³ *Cefalu v. Globe Newspaper Co.*, 391 N.E.2d 935, 939 (Mass. App. Ct. 1979).

³⁰⁴ 469 N.E.2d 1025, 1028 (Ohio Ct. App. 1984) (quoting *Jackson v. Playboy Enters.*, 574 F. Supp. 10, 13 (S.D. Ohio 1983)).

³⁰⁵ 201 Cal. Rptr. 665, 666 (Ct. App. 1984).

³⁰⁶ *Id.* at 669 ("[P]rior to the publication of the newspaper articles in question [Sipple]'s homosexual orientation and participation in gay community activities had been known by hundreds of people in a variety of cities . . .").

³⁰⁷ 504 N.W.2d 715, 718 (Mich. Ct. App. 1993).

few - but not all

she had revealed it to a few people.³⁰⁸ A few courts, however, have come to different conclusions regarding whether there is a privacy interest in information communicated to others. For example, in *Times Mirror Co. v. Superior Court*, the identity of a murder witness was disclosed in a newspaper article.³⁰⁹ Although the witness had confided in a few friends and family members, she had not “rendered otherwise private information public by cooperating in the criminal investigation and seeking solace from friends and relatives.”³¹⁰

Lior Strahilevitz aptly observes that disclosure involves spreading information beyond existing networks of information flow.³¹¹ The harm of disclosure is not so much the elimination of secrecy as it is the spreading of information beyond expected boundaries. People often disclose information to a limited circle of friends, and they expect the information to stay within this group. Some courts, however, focus on secrecy and do not examine people’s expectations of information flow.³¹²

3. Exposure

In an 1881 case, *DeMay v. Roberts*, a young unmarried man accompanied a doctor into the room where the doctor was assisting a woman in labor.³¹³ The court held that the young man had no business being in the room: “It would be shocking to our sense of right, justice and propriety to doubt even but that for such an act the law would afford an ample remedy.”³¹⁴ Why is it “shocking” for a stranger to watch a woman give birth to a baby?

³⁰⁸ *Id.* at 720 (finding her identity to be “open to the public eye” because her work in Colombia had been disclosed in newspaper articles, and because she had occasionally used her real name in the United States); see also *Fisher v. Ohio Dep’t of Rehab. & Corr.*, 578 N.E.2d 901, 903 (Ohio Ct. Cl. 1988) (holding that the disclosure of a public conversation between a plaintiff and her fellow employees was not a privacy violation).

³⁰⁹ 244 Cal. Rptr. 556, 558 (Ct. App. 1988).

³¹⁰ *Id.* at 561; see also *Multimedia WMAZ, Inc. v. Kubach*, 443 S.E.2d 491, 500 (Ga. Ct. App. 1994) (finding that the plaintiff’s disclosure of his infection status to family, friends, and members of an HIV support group did not render the information public); *Y.G. v. Jewish Hosp.*, 795 S.W.2d 488, 500 (Mo. Ct. App. 1990) (holding that disclosure to doctors and other participants of the plaintiff’s in vitro fertilization did not render that information public).

³¹¹ See Lior Jacob Strahilevitz, *A Social Networks Theory of Privacy*, 72 U. CHI. L. REV. 919, 974 (2005) (arguing that an individual has a reasonable expectation of privacy where there is a low risk that the information will spread beyond the individual’s social network).

³¹² See *id.* at 943-45 (describing “hard-line” cases in which plaintiffs’ limited disclosures barred their privacy claims).

³¹³ 9 N.W. 146, 146 (Mich. 1881).

³¹⁴ *Id.* at 148-49.

In 2004, in *National Archives & Records Administration v. Favish*, the Supreme Court rejected a request under the Freedom of Information Act (FOIA) for autopsy photos of Vincent Foster, Jr., a deputy counsel to President Clinton who had committed suicide by shooting himself.³¹⁵ The Court concluded that the photos fell under the exemption for records that "could reasonably be expected to constitute an unwarranted invasion of personal privacy."³¹⁶ The Court contended: "Family members have a personal stake in honoring and mourning their dead and objecting to unwarranted public exploitation that, by intruding upon their own grief, tends to degrade the rites and respect they seek to accord to the deceased person who was once their own."³¹⁷

Why is it indecent to publish autopsy photographs? What harm does it cause the families? Imagine that a newspaper prints candid photographs of a person naked or of a person defecating. The person would likely be appalled. But why? We all have genitals. We all defecate. There are no big surprises here.

These are all illustrations of a disruption I call "exposure." Exposure involves the exposing to others of certain physical and emotional attributes about a person. These are attributes that people view as deeply primordial, and their exposure often creates embarrassment and humiliation. Grief, suffering, trauma, injury, nudity, sex, urination, and defecation all involve primal aspects of our lives—ones that are physical, instinctual, and necessary.³¹⁸ We have been socialized into concealing these activities.³¹⁹

Although exposure is similar to disclosure—both involve the dissemination of true information—they diverge in an important respect. Exposure is related to disclosure in that concealed information is revealed to others, but the information is not revealing of anything we typically use to judge people's character. Unlike disclosure, exposure rarely reveals any signifi-

³¹⁵ 541 U.S. 157, 175 (2004).

³¹⁶ *Id.* at 171 (quoting 5 U.S.C. § 552(b)(7)(C) (2000))(internal quotation marks omitted).

³¹⁷ *Id.* at 168. Courts have also allowed tort suits based on the dissemination of autopsy photos. See *Reid v. Pierce County*, 961 P.2d 333, 339-42 (Wash. 1998) (en banc) (holding that relatives of deceased persons maintained a cause of action for invasion of privacy when coroner's office employees disseminated autopsy photos).

³¹⁸ See, e.g., Anita L. Allen, *Lying to Protect Privacy*, 44 VILL. L. REV. 161, 177 (1999) ("Sex is an area in which we encounter our desires, prejudices and shame, and cloak these emotions in privacy.").

³¹⁹ See NORBERT ELIAS, *THE CIVILIZING PROCESS* 114 (Edmund Jephcott trans., 1994) (1939) ("The social reference of shame and embarrassment recedes more and more from consciousness. Precisely because the social command not to show oneself exposed or performing natural functions now operates with regard to everyone[,] . . . it seems to the adult a command of his own inner self . . .").

bl

Cultural
norms

↓
img rare

↓
so shocking

cant new information that can be used in the assessment of a person's character or personality.

Exposure creates injury because we have developed social practices to conceal aspects of life that we find animal-like or disgusting. Further, in certain activities, we are vulnerable and weak, such as when we are nude or going to the bathroom. Norms about nudity and bodily functions have changed throughout history.³²⁰ Martha Nussbaum points out that ancient Romans used toilets whereas "courtiers in Elizabethan England urinated and defecated in corners of palaces, until the stench made it necessary to change residences."³²¹ In various cultures and at different times in history, levels of reticence and modesty concerning the body have differed greatly.³²² Today's norms and practices, however, call for the concealment of many aspects of the body, bodily functions, and strong displays of emotion. We protect against the exposure of these bodily aspects because this protection safeguards human dignity as defined by modern society. Dignity is a part of being civilized; it involves the ability to transcend one's animal nature.³²³

The need for privacy, and therefore the prevention of exposure, is created by the fact that we have social relationships and concomitant norms of dignity and decorum.³²⁴ "The private arises as a necessary space for the production of civilized behavior," William Ian Miller contends.³²⁵ "Private space enables a civilized public space."³²⁶

³²⁰ See Solove, *Conceptualizing Privacy*, *supra* note 11, at 1135-36 (observing that public bathing was common in the Middle Ages, but that by the sixteenth century concealment of the body had become the norm).

³²¹ MARTHA C. NUSSBAUM, *HIDING FROM HUMANITY: DISGUST, SHAME, AND THE LAW* 115-16 (2004).

³²² See Solove, *Conceptualizing Privacy*, *supra* note 11, at 1135-36 (comparing ancient Greece, where public nudity was seen as a sign of strength, to Renaissance Europe, where "among the wealthy . . . people tried to distance themselves from their body and other's bodies").

³²³ See WILLIAM IAN MILLER, *THE ANATOMY OF DISGUST* 177 (1997) ("The civilizing process, according to [Norbert] Elias, means the expansion of the private sphere at the expense of the public. The new norms demand private spaces in which one prepares, grooms, and does the things that would disgust others if they were to be witnessed."); CARL D. SCHNEIDER, *SHAME, EXPOSURE, AND PRIVACY* 49 (W.W. Norton 1992) (1977) ("The open display of bodily functions—defecating, great pain, the process of dying—threatens the dignity of the individual, revealing an individual vulnerable to being reduced to his bodily existence, bound by necessity.").

³²⁴ Certain activities, such as defecation, we view as uncivilized to perform in front of others. As William Ian Miller observes: "Clearly defecation is degrading and contaminating. It is hedged in with rules about appropriateness as to place. And to violate those rules is a cause for disgrace and shame . . ." MILLER, *supra* note 323, at 147 (footnote omitted).

³²⁵ *Id.* at 178.

³²⁶ *Id.*

When these practices are disrupted by exposure, people can experience a severe and sometimes debilitating humiliation and loss of self-esteem. Exposure thus impedes a person's ability to participate in society. Even though most people would not view a victim of exposure as a lesser person or as being less civilized, victims feel that way. This is in contrast to disclosure, where information often alters the way a person is perceived.

Disclosure is a power that controls through the imposition of social sanctions and condemnation. Exposure works in a different way, by stripping people of their dignity.³²⁷ Exposure interacts with powerful and potent social norms. When people willingly transgress these norms, society has a strong interest in shaming them, and it is socially beneficial for these norms to be internalized and to result in feelings of shame. However, exposure involves people unwillingly placed in transgression of these norms. We do not view the victims as blameworthy, and there is little social value in their suffering. Nevertheless, due to the internalization of these norms, exposure victims experience strong feelings of shame.

Tort law does not recognize a separate cause of action for exposure; the tort of public disclosure covers both disclosure and exposure.³²⁸ Generally, exposure cases have fared better than ones involving disclosure.³²⁹ For example, in *Daily Times Democrat v. Graham*, air jets blew up a woman's dress while she was at a county fair, exposing her underwear.³³⁰ At that very moment, a photographer for the local newspaper took her photograph, and the picture was printed on the front page of the paper.³³¹ The woman sued under the public disclosure tort.³³² The newspaper contended that the picture was taken in public, and that, accordingly, there was no privacy interest.³³³ This reasoning was based on the secrecy paradigm—that once something is disclosed to the public, it is no longer secret. However, the court concluded that the woman still had a right to be protected from “an

³²⁷ One victim of Chicago's invasive strip search policy testified that “the incident caused her emotional distress that manifested itself in reduced socializing, poor work performance, paranoia, suicidal feelings, depression, and an inability to disrobe in any place other than a closet.” *Joan W. v. City of Chicago*, 771 F.2d 1020, 1021-22 (7th Cir. 1985).

³²⁸ RESTATEMENT (SECOND) OF TORTS, § 652D (1977).

³²⁹ Eugene Volokh explains that this difference may be because the information revealed via exposure is less useful to those to whom the information is given than that revealed via disclosure. Volokh, *supra* note 287, at 1094.

³³⁰ 162 So. 2d 474, 476 (Ala. 1964).

³³¹ *Id.*

³³² *Id.* at 476-77.

³³³ *Id.* at 477.

indecent and vulgar" violation of privacy under the tort of public disclosure.³³⁴

Failing to distinguish between disclosure and exposure has adversely affected the recognition of exposure harms in some instances. In *McNamara v. Freedom Newspapers, Inc.*, for example, a newspaper published a picture of a high school athlete whose genitalia was accidentally exposed while playing soccer.³³⁵ The student sued under the tort of public disclosure of private facts.³³⁶ According to the student, "the Newspaper violated the bounds of public decency."³³⁷ The court conceptualized the injury as one of disclosure and concluded that the picture was not private because "[the student] was voluntarily participating in a spectator sport at a public place."³³⁸ The harm in this case, however, is more appropriately classified as one of exposure. Had the court conceptualized the disruption as one of exposure, the fact that it occurred in a public place would have been much less relevant to the analysis.

4. Increased Accessibility

The federal courts, along with many state courts and agencies, are developing systems to place their records online.³³⁹ These records are readily available at local courthouses or government offices. Nevertheless, placing them online has given rise to an extensive debate over privacy. Some argue that the information is already publicly available, and that therefore it should be available on the Internet in the same manner as it is in physical form at the localities. But many administrative bodies charged with examining the issue have hesitated because of the increased accessibility the Internet will bring. The federal Judicial Conference Committee concluded, for example, that "any benefits of public remote electronic access to criminal files were outweighed by the safety and law enforcement risks such access would create."³⁴⁰

³³⁴ *Id.* at 478.

³³⁵ 802 S.W.2d 901, 903 (Tex. App. 1991).

³³⁶ *Id.*

³³⁷ *Id.* at 905.

³³⁸ *Id.*

³³⁹ See SOLOVE, THE DIGITAL PERSON, *supra* note 40, at 131-32 (observing that digital filing requirements and the conversion of paper files to digital format will lead to significant online accessibility of court records).

³⁴⁰ JUDICIAL CONFERENCE COMM. ON COURT ADMIN. AND CASE MGMT., REPORT ON PRIVACY AND PUBLIC ACCESS TO ELECTRONIC CASE FILES (2001), <http://www.privacy.uscourts.gov/Policy.htm>.

If the information is already available to the public, then what is the harm in increasing its accessibility? Increased accessibility does not involve a direct disclosure. Secret information is not disclosed. Rather, information that is already available to the public is made easier to access. Unlike disclosure, the harm is not a direct revealing of information to another. Confidentiality is not breached; the cat is already out of the bag. With increased accessibility, a difference in quantity becomes a difference in quality—it enhances the risk of the harms of disclosure.

Increased accessibility to personal information has many benefits. It enhances openness, allowing people to locate information that they are seeking more easily. Ready accessibility of records enables attorneys to track down people's addresses to serve process. It can assist in investigating the background of a person that one is planning to hire as a child caregiver or teacher. As Robert Gellman notes: "Some basic functions and institutions depend on the public availability of records to operate. The U.S. system of land ownership relies on the public availability of records, although that has not always been the case. The public availability of bankruptcy records is also integral to the process."³⁴¹

Increased accessibility, however, creates problems such as the increased possibility of disclosure. Information can readily be exploited for purposes other than those for which it was originally made publicly accessible. For example, companies are gathering data from public records to use for commercial and marketing purposes or to create dossiers on individuals for profiling and other analysis.³⁴² As Peter Winn notes, increased access to court records will cause harms to participants in the judicial system: "They will lose . . . their interest in privacy—their identities will be subject to potential misuse by thieves, and their children may be exposed to sexual predators."³⁴³

Under the secrecy paradigm, courts often view privacy as a binary status—information is either completely private or completely public.³⁴⁴ Accordingly, once information is released into the public domain, it is no longer private. According to the Restatement, for the tort of public disclosure, "[t]here is no liability when the defendant merely gives further public-

It actually makes a huge diff

³⁴¹ Robert Gellman, *Public Records, Public Policy, and Privacy*, HUMAN RTS., Winter 1999, at 7, 9.

³⁴² SOLOVE, THE DIGITAL PERSON, *supra* note 40, at 131-32; see also Gellman, *supra* note 341, at 7 (warning that although "[p]rivacy protections were inherent in the technology of paper," digitization has led to increased accessibility).

³⁴³ Peter A. Winn, *Online Court Records: Balancing Judicial Accountability and Privacy in an Age of Electronic Information*, 79 WASH. L. REV. 307, 315 (2004).

³⁴⁴ See *supra* notes 90-91 and accompanying text for an explanation of the secrecy paradigm.

ity to information about the plaintiff that is already public."³⁴⁵ For the harm of increased accessibility, however, prior publicity is not dispositive. One must focus on the extent to which the information is made more accessible. Most courts, however, due to their commitment to the secrecy paradigm, struggle with recognizing this harm.³⁴⁶ In *Walls v. City of Petersburg*, for example, public employees were compelled to answer a questionnaire asking about the criminal histories of their family members, their complete marital history, their children, and their financial status.³⁴⁷ The court dismissed their claim that their constitutional right to information privacy was violated, reasoning that there was no privacy interest in the information because it was already available in public records.³⁴⁸

In *United States Department of Justice v. Reporters Committee for Freedom of the Press*, the Supreme Court recognized the problem of increased accessibility.³⁴⁹ Earlier in this Article, I noted how this case also recognized the problem of aggregation when the Court concluded that the disclosure of FBI "rap sheets" violated a cognizable privacy interest under FOIA.³⁵⁰ In addition to concluding that there was a difference between scattered pieces of information and a fully assembled dossier, the Court recognized that "there is a vast difference between the public records that might be found after a diligent search of courthouse files, county archives, and local police stations throughout the country and a computerized summary located in a single clearinghouse of information."³⁵¹ Here, the Court has recognized the harm of increased accessibility.³⁵²

³⁴⁵ RESTATEMENT (SECOND) OF TORTS § 652D cmt. b (1977).

³⁴⁶ See, e.g., *Cline v. Rogers*, 87 F.3d 176, 179 (6th Cir. 1996) (holding that the constitutional right to information privacy did not apply to the disclosure of police records because "one's criminal history is arguably not a private 'personal matter' at all, since arrest and conviction information are matters of public record"); *Doe v. City of New York*, 15 F.3d 264, 268-69 (2d Cir. 1994) (finding that "an individual cannot expect to have a constitutionally protected privacy interest in matters of public record" but that plaintiff's HIV status was not a matter of public record); *Scheetz v. Morning Call, Inc.*, 946 F.2d 202, 207 (3d Cir. 1991) (holding that because information about the victim's claims of spousal abuse potentially "would have wound up on the public record," the victim did not have a privacy interest in the claims).

³⁴⁷ 895 F.2d 188, 190 (4th Cir. 1990).

³⁴⁸ *Id.* at 193-94.

³⁴⁹ See 489 U.S. 749, 780 (1989) (observing that the "practical obscurity" of a rap sheet is an important element in personal privacy).

³⁵⁰ See *supra* notes 151-56 and accompanying text.

³⁵¹ *Reporters Comm.*, 489 U.S. at 764.

³⁵² *Id.* at 780.

5. Blackmail

In nineteenth-century England, sodomy was a serious offense. Although no longer a capital offense—as it had been in the seventeenth century—sodomy still carried harsh penalties from ten years to life in prison.³⁵³ Blackmailers would threaten wealthy elites with disclosure of their homosexual activities unless the blackmailers were paid handsomely. The law began to recognize that such forms of extortion should be criminalized. When a blackmail case came to court, courts would awkwardly ignore whether there was any truth to the blackmailer's charges.³⁵⁴ Certainly not all victims of blackmail were innocent, yet courts offered protection even to those accused of transgressing society's strong sexual taboos and criminal laws. Why were such people protected? If the society so vehemently condemned sodomy at the time, why punish the blackmailers rather than those who may have been guilty of sodomy?

One nineteenth-century English judge contended that blackmail was "one of the worst offenses known to the law."³⁵⁵ As historian Angus McLaren notes:

The courts had for centuries reassured the [wealthy] that their good names were protected by the laws on libel and slander. The publicity given to the emergence of the blackmailer raised the horrific possibility that the pillaging of the propertied could be carried out by those who threatened not to tell hurtful lies, but obscene truths.³⁵⁶

Blackmail has long posed a conundrum for legal scholars.³⁵⁷ Blackmail involves coercing an individual by threatening to expose her personal secrets if she does not accede to the demands of the blackmailer, which often involve paying hush money.³⁵⁸ Why should society restrict contracts not to

³⁵³ ANGUS McLAREN, *SEXUAL BLACKMAIL* 17 (2002) (noting that there were no executions for sodomy in England after 1836).

³⁵⁴ See *id.* at 21 (explaining that "[v]ictims who appeared to have engaged in same-sex activities put the courts in a potentially awkward situation," as the courts did not want to exonerate those who had engaged in same-sex activities).

³⁵⁵ *Id.* at 20 (quoting *Central Criminal Court*, *TIMES* (London), June 20, 1895, at 3).

³⁵⁶ *Id.* at 28-29.

³⁵⁷ See LEO KATZ, *ILL GOTTEN GAINS* 140-45 (1996) (discussing various philosophers' interpretations of the connection between blackmail and coercion and the difficulties of formulating a complete theory). The term "blackmail" originated in Tudor times and referred to extortion in general. McLAREN, *supra* note 353, at 12. "Modern blackmail first emerged when criminals in the eighteenth century recognized that the laws against sodomy provided them with the means by which they could extort money from those whom they could entrap." *Id.* at 3.

³⁵⁸ See 31A AM. JUR. 2D, *Extortion, Blackmail, and Threats* § 20 (2002) (recognizing that, although statutes differ in form, the use of a threat to extract something is at the heart of blackmail). For a discussion of how blackmail laws protected reputations in different periods

divulge secrets? Blackmail does not seem to be about preventing disclosure, for as Joseph Izenberg argues, prohibiting a blackmailer compensation for silence will likely make disclosure more probable.³⁵⁹ If this is the case, then what interest does the crime of blackmail protect?

Scholars have offered a panoply of hypotheses. Richard Posner argues that blackmail is illegal because it neither maximizes wealth nor provides any net social benefit.³⁶⁰ In contrast, Gary Anderson and Walter Block contend that blackmail, as distinct from extortion, involves a transaction just like any other, in which both parties bargain for the result they desire.³⁶¹ Jennifer Brown finds that blackmail undermines the criminal justice system by enabling private contracts that withhold information from the justice system.³⁶² Richard Epstein proposes that blackmail is socially detrimental because it "breeds fraud and deceit."³⁶³ According to Wendy Gordon, blackmail is illegal because it involves the blackmailer treating the victim as a means (to earn money) rather than an end.³⁶⁴ Finally, Richard McAdams argues that blackmail inhibits the development of social norms by stifling public norm enforcement and the discussion and critique of norms.³⁶⁵

I posit that blackmail is criminalized because of the power relationship it creates. Blackmail allows a person to be dominated and controlled by another. With blackmail, the harm is not in the actual disclosure of the information, but in the control exercised by the one who makes the threat over the data subject. In some cases, blackmail can also involve information more akin to exposure than disclosure. Breach of confidentiality is also related to blackmail, as a confidant can threaten to disclose a secret in return

nice

of American history, see Lawrence M. Friedman, *Name Robbers: Privacy, Blackmail, and Assorted Matters in Legal History*, 30 HOFSTRA L. REV. 1093, 1112-13 (2002) (observing that blackmail went "against the American grain" of allowing second chances and fresh starts).

³⁵⁹ Joseph Isenbergh, *Blackmail From A to C*, 141 U. PA. L. REV. 1905, 1914 (1993) (noting that in any given case, individuals who have obtained valuable information are most likely to disclose it in the presence of a law forbidding bargaining for secrecy with data subjects, though in the long run, such laws will deter potential blackmailers from digging for valuable information).

³⁶⁰ Richard A. Posner, *Blackmail, Privacy, and Freedom of Contract*, 141 U. PA. L. REV. 1817, 1818-20 (1993).

³⁶¹ Walter Block & Gary M. Anderson, *Blackmail, Extortion and Exchange*, 44 N.Y.L. SCH. L. REV. 541, 544-47 (2001).

³⁶² Jennifer Gerarda Brown, *Blackmail as Private Justice*, 141 U. PA. L. REV. 1935, 1971 (1993).

³⁶³ Richard A. Epstein, *Blackmail, Inc.*, 50 U. CHI. L. REV. 553, 565 (1983).

³⁶⁴ Wendy J. Gordon, *Truth and Consequences: The Force of Blackmail's Central Case*, 141 U. PA. L. REV. 1741, 1761 (1993).

³⁶⁵ Richard H. McAdams, *Group Norms, Gossip, and Blackmail*, 144 U. PA. L. REV. 2237, 2243-64 (1996).

for money. Blackmail differs from disclosure, exposure, and breach of confidentiality in that it involves a threat of disclosure rather than an actual disclosure.

A rough analogy may be made to the crimes of battery and assault. Battery involves actual physical harm, whereas assault is putting a person in fear of physical harm.³⁶⁶ But there are important differences between blackmail and assault. Unlike assault, where the violence threatened is illegal, with blackmail, the threatened disclosure can be perfectly legal. Indeed, the disclosure might be socially beneficial in that it might reveal that the blackmail victim committed a crime or heinous act. But the threat of disclosure is so profoundly disempowering that society still wants to protect against it. Toward the end of Henrik Ibsen's play, *Hedda Gabler*, Judge Brack, who knows a damaging secret about Hedda Gabler, says to her, "My dearest Hedda, believe me I shall not abuse the position." Hedda replies, "In your power, all the same. At the mercy of your will and demands. And so a slave! A slave!"³⁶⁷ The more people know about us, the more they can exercise control over us. This is why telling one's deepest secrets to another makes one vulnerable. Prohibiting blackmail prevents people from taking advantage of us with our personal information.

The purpose of restricting blackmail is not to limit disclosure but to prevent the use of the threat of disclosure as a tool for exerting power and dominion over others. Our society prohibits slavery, labor below the minimum wage, dangerous workplace conditions, and quid pro quo sexual harassment even if the victim seemingly consents. The rationale for these prohibitions stems in part from the fact that these acts are so coercive that the consent is not voluntary, and so place excessive power over one person in the hands of another. Blackmail similarly demonstrates the profound danger of the threat of disclosure as an instrument of power over another person. Indeed, criminal codes classify blackmail as a form of extortion, which involves the use of fear or threats to force someone to submit to another's will.³⁶⁸

The crime of blackmail thus prevents the use of disclosure, exposure, or breach of confidentiality as a means for exercising power over another person. Dissemination of information is a powerful tool, one that can be

³⁶⁶ See RESTATEMENT (SECOND) OF TORTS § 13 (1965) (defining battery); *id.* § 21 (defining assault).

³⁶⁷ HENRIK IBSEN, *Hedda Gabler*, in *HEDDA GABLER AND OTHER PLAYS* 362 (Una Ellis-Fermor trans., Penguin Books 1961).

³⁶⁸ See, e.g., CAL. PENAL CODE § 518 (West 1999) (defining extortion as "the obtaining of property from another, with his consent, or the obtaining of an official act of a public officer, induced by a wrongful use of force or fear").

wielded to achieve levels of domination and control that may not be socially beneficial. This is why the threats are usually treated as part of the wrongful act itself.

6. Appropriation

In 1902, in *Roberson v. Rochester Folding Box Co.*, a flour company included a lithograph of Abigail Roberson, a minor, on 25,000 advertisement flyers without her consent.³⁶⁹ The flyers were captioned, "Flour of the Family."³⁷⁰ Roberson alleged that she "ha[d] been greatly humiliated by the scoffs and jeers of persons who ha[d] recognized her face and picture on this advertisement, and her good name ha[d] been attacked, causing her great distress and suffering, both in body and mind."³⁷¹ The portrait, however, was neither racy nor libelous. "The likeness is said to be a very good one," the court noted, and Roberson was "caused to suffer mental distress where others would have appreciated the compliment to their beauty implied in the selection of the picture for such purposes."³⁷² The court refused to recognize a remedy based on Warren and Brandeis's article, concluding that such an action was the proper domain of the legislature.³⁷³

Roberson caused quite a stir. An editorial in *The New York Times* lambasted the decision and noted that it "excited as much amazement among lawyers and jurists as among the promiscuous lay public."³⁷⁴ Shortly after the decision, a comment in the *Yale Law Journal* criticized the *Roberson* decision for not recognizing a remedy for the "undoubted injury to the plaintiff."³⁷⁵ The strong criticism of the decision even led one of the judges of the majority to defend the opinion in the *Columbia Law Review*.³⁷⁶ A year later, New York passed a law creating a cause of action to redress the type of injury Roberson suffered.³⁷⁷ The law still remains viable today.³⁷⁸

³⁶⁹ 64 N.E. 442, 442 (N.Y. 1902).

³⁷⁰ *Id.*

³⁷¹ *Id.* Roberson became so ill that she had to see a physician. *Id.*

³⁷² *Id.* at 442-43.

³⁷³ *Id.* at 447-48 (applying Warren & Brandeis, *supra* note 21).

³⁷⁴ Editorial, *The Right of Privacy*, N.Y. TIMES, Aug. 23, 1902, at 8, reprinted in Denis O'Brien, *The Right of Privacy*, 2 COLUM. L. REV. 437, 438 (1902).

³⁷⁵ Comment, *An Actionable Right to Privacy?: Roberson v. Rochester Folding Box Co.*, 12 YALE L.J. 35, 36 (1902).

³⁷⁶ O'Brien, *supra* note 374, at 437.

³⁷⁷ See, e.g., Irwin R. Kramer, *The Birth of Privacy Law: A Century Since Warren and Brandeis*, 39 CATH. U. L. REV. 703, 717 (1990) (noting that the statutes "made it both a tort and a misdemeanor . . . to use another's name, portrait, or picture for commercial purposes without the subject's consent").

³⁷⁸ N.Y. CIV. RIGHTS LAW §§ 50, 51 (McKinney 1992).

The tort of appropriation was thus one of the first privacy torts to be recognized after Warren and Brandeis's article. The tort of appropriation occurs when "[o]ne . . . appropriates to his own use or benefit the name or likeness of another."³⁷⁹ To be liable for appropriation, "the defendant must have appropriated to his own use or benefit the reputation, prestige, social or commercial standing, public interest or other values of the plaintiff's name or likeness."³⁸⁰

FB Beacon

Why did *Roberson* create such a response? What spurred such an extensive public discussion and prompt legislative action? What is problematic about using a person's name or photograph in an advertisement? After all, one's name and image are often not secret. The picture of *Roberson* was flattering and did not ruin her reputation. What was the injury?

"Appropriation" is the use of one's identity or personality for the purposes and goals of another. Appropriation, like the privacy disruptions of disclosure and distortion, involves the way an individual desires to present herself to society.

The tort of appropriation has currently lost its way, as courts and commentators have not been able to adequately explain the injury that is redressed by the tort. Two competing accounts of the injury predominate in cases and commentary.³⁸¹ Many commentators describe the harm caused by the use of one's likeness for commercial purposes as an affront to dignity; Edward Bloustein argued that the harm caused to an individual by appropriation is the "demeaning and humiliating . . . commercialization of an aspect of personality."³⁸²

Another rationale for the tort is as a protection of property rights. Prosser, who was profoundly influential in the creation of the four modern privacy torts, viewed the interest protected by the appropriation tort as "not so much a mental as a proprietary one."³⁸³ According to Jonathan Kahn, the "early association of appropriation claims with such intangible, non-commensurable attributes of the self as dignity and the integrity of one's persona seems to have been lost, or at least misplaced, as property-based conceptions of the legal status of identity have come to the fore."³⁸⁴ Courts

³⁷⁹ RESTATEMENT (SECOND) OF TORTS § 652C (1977).

³⁸⁰ *Id.* § 652C cmt. c.

³⁸¹ See generally Robert C. Post, *Rereading Warren and Brandeis: Privacy, Property, and Appropriation*, 41 CASE W. RES. L. REV. 647 (1991) (contrasting the "property" and "dignity" rationales for the tort of appropriation).

³⁸² Edward J. Bloustein, *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser*, 39 N.Y.U. L. REV. 962, 987 (1964).

³⁸³ Prosser, *supra* note 20, at 406.

³⁸⁴ Jonathan Kahn, *Bringing Dignity Back to Light: Publicity Rights and the Eclipse of the Tort of Appropriation of Identity*, 17 CARDOZO ARTS & ENT. L.J. 213, 223 (1999). A new

have transformed a tort's targeted harm from one of appropriation to one of intellectual property. Most contemporary cases recognize that the tort of appropriation protects a "valuable right of property."³⁸⁵ Loss of property seems to be more readily recognized by courts today than the more amorphous feelings of embarrassment or loss of dignity.³⁸⁶

To the extent that the tort remains a way to protect against the loss of dignity, why should we inhibit social use of identities simply to prevent people from feeling demeaned when their identities are commercialized? After all, we allow people to sell their identities to endorse products. Further, we allow vigorous criticism and satire, which can be quite humiliating and injurious to people's dignity.

I contend that there is another important dimension of the harm of appropriation—an interference with freedom and self-development. The early appropriation cases allude to this aspect of the harm. In 1905, Georgia became the first state to recognize a tort based on Warren and Brandeis's article. In *Pavesich v. New England Life Insurance Co.*, a life insurance advertisement used a photograph of Paolo Pavesich next to a photograph of "an ill-dressed and sickly looking person."³⁸⁷ Under Pavesich's picture, the advertisement stated in part: "In my healthy and productive period of life I bought insurance in the New England Mutual Life Insurance Co."³⁸⁸ The ad seemed flattering for Pavesich, for he was the paragon of all the success and good fortune that would come to those who purchased insurance.³⁸⁹ Pavesich, however, was not flattered, and he sued.³⁹⁰ In contrast to the *Roberson* court, the *Pavesich* court recognized a cause of action, reasoning that "the body of a person cannot be put on exhibition . . . without his consent. The right of one to exhibit himself to the public at all proper times, in all proper

model releases

tort, known as the "right of publicity," has emerged to redress violations of property rights in one's name or likeness. See, e.g., 1 MCCARTHY, *supra* note 3, § 5:63 ("Simplistically put, while the appropriation branch of the right of privacy is invaded by an injury to the psyche, the right of publicity is infringed by an injury to the pocketbook." (footnote omitted)).

³⁸⁵ DAVID A. ELDER, *THE LAW OF PRIVACY* § 6:1, at 375 (1991) (quoting *McQueen v. Wilson*, 161 S.E.2d 63, 66 (Ga. Ct. App.), *rev'd on other grounds*, 162 S.E.2d 313 (Ga. 1968)).

³⁸⁶ See Andrew J. McClurg, *A Thousand Words Are Worth a Picture: A Privacy Tort Response to Consumer Data Profiling*, 98 NW. U. L. REV. 63, 109, 114 (2003) (arguing that Prosser's characterization of appropriation as vindicating property interests obscured the dignity interests the tort protected, and noting that "[m]odern courts are prone to subsuming the privacy claim under the label of publicity").

³⁸⁷ 50 S.E. 68, 68 (Ga. 1905).

³⁸⁸ *Id.* at 69.

³⁸⁹ *Id.*

³⁹⁰ *Id.*

places, and in a proper manner is embraced within the right of personal liberty."³⁹¹ The use of one's likeness for advertising purposes can bring

even the individual of ordinary sensibility[] to a realization that his liberty has been taken away from him; and, as long as the advertiser uses him for these purposes, he cannot be otherwise than conscious of the fact that he is for the time being under the control of another, that he is no longer free, and that he is in reality a slave.³⁹²

The court speaks in terms of loss of liberty, not in terms of loss of monetary value. The injury is that Pavesich has been used against his will. Similarly, according to Justice Gray's dissent in *Roberson*, "we may not say that the plaintiff's complaint is fanciful, or that her alleged injury is purely a sentimental one."³⁹³ "[T]he conspicuous display of her likeness in various public places has . . . humiliated her by the notoriety and by the public comments it has provoked."³⁹⁴ Justice Gray alluded to what I believe to be the crux of the harm: unwanted notoriety. The appropriation of *Roberson's* image forced her to become a public figure. In addition to bringing her unwillingly into the public sphere, the appropriation defined her public role and public persona.

The interest safeguarded by protections against appropriation is control of the way one presents oneself to society. The products and causes people publicly endorse shape their public image. When people are associated with products, they become known in terms of these products. Many public figures take great care with their endorsements because these endorsements shape their public image.³⁹⁵ Thus, appropriation can be harmful even if it is not humiliating, degrading, or disrespectful. Being unwillingly used to endorse a product resembles, in certain respects, being compelled to speak and to represent certain viewpoints.

Protection against appropriation establishes what society considers appropriate for others to do in shaping a person's identity. The harm, then, is

³⁹¹ *Id.* at 70.

³⁹² *Id.* at 80.

³⁹³ *Roberson v. Rochester Folding Box Co.*, 64 N.E. 442, 449 (N.Y. 1902) (Gray, J., dissenting).

³⁹⁴ *Id.*

³⁹⁵ For example, in 1903, Thomas Edison sought to enjoin the Edison Polyform Manufacturing Company from using his picture on bottles of a pain reliever that Edison himself had invented earlier in his career. *Edison v. Edison Polyform Mfg. Co.*, 67 A. 392, 392 (N.J. Ch. 1907). The court granted the injunction. *Id.* at 395. Similarly, Jacqueline Onassis sued a clothing company for the use of a lookalike in an advertisement because "she has never permitted her name or picture to be used in connection with the promotion of commercial products. Her name has been used sparingly only in connection with certain public services, civic, art and educational projects which she has supported." *Onassis v. Christian Dior—New York, Inc.*, 472 N.Y.S.2d 254, 257 (Sup. Ct. 1984).

an impingement on the victim's freedom in the authorship of her self-narrative, not merely her loss of profits. Prosser, however, used the term "appropriation," which is a word that pertains to property. Perhaps a better word to describe the harm is "exploitation." I continue to use the word appropriation, however, because it has become so commonly known in relation to this kind of harmful activity.

7. Distortion

Defamation law has existed for centuries. Consisting of the torts of libel and slander, defamation law protects against falsehoods that injure a person's reputation. In order to be liable for defamation, one must make "a false and defamatory statement concerning another."³⁹⁶ A "defamatory" statement "tends so to harm the reputation of another as to lower him in the estimation of the community or to deter third persons from associating or dealing with him."³⁹⁷ False light, a more recent tort inspired by the Warren and Brandeis article,³⁹⁸ protects against giving "publicity to a matter concerning another that places the other before the public in a false light" that is "highly offensive to a reasonable person."³⁹⁹ It safeguards "the interest of the individual in not being made to appear before the public in an objectionable false light or false position, or in other words, otherwise than as he is."⁴⁰⁰ False light is categorized as one of Prosser's four "privacy" torts.⁴⁰¹

In addition to false light and defamation, a number of privacy statutes ensure accuracy in record systems. The Privacy Act, for example, enables a person to access and correct her records maintained by government agencies.⁴⁰² Likewise, the Fair Credit Reporting Act provides recourse for a person who wants to correct her credit records,⁴⁰³ and the Family Educational Rights and Privacy Act enables students to review and ensure the accuracy of their school records.⁴⁰⁴ Additionally, longstanding privacy principles,

³⁹⁶ RESTATEMENT (SECOND) OF TORTS § 558(a) (1977).

³⁹⁷ *Id.* § 559.

³⁹⁸ See, e.g., Gary T. Schwartz, *Explaining and Justifying a Limited Tort of False Light Invasion of Privacy*, 41 CASE W. RES. L. REV. 885, 885 (1991) (noting that the Warren and Brandeis article led to decisions which Prosser later labeled as the false light tort).

³⁹⁹ RESTATEMENT (SECOND) OF TORTS § 652E. Although there is a significant amount of overlap between the two torts, false light has a more expansive view of the harm caused by distortion. While defamation requires the proof of reputational harm, false light does not, and plaintiffs can be compensated solely for emotional distress. Schwartz, *supra* note 398, at 887.

⁴⁰⁰ RESTATEMENT (SECOND) OF TORTS § 652E cmt. b.

⁴⁰¹ Prosser, *supra* note 20, at 389.

⁴⁰² 5 U.S.C. § 552a(d) (2000).

⁴⁰³ 15 U.S.C. § 1681i (2000).

⁴⁰⁴ 20 U.S.C. § 1232g(a)(2) (2000).

arbitrary
broad statement
at first
now closely
read

such as the Code of Fair Information Practice⁴⁰⁵ and the Organization for Economic Cooperation and Development (OECD) Privacy Guidelines, contain provisions for ensuring the accuracy of records.⁴⁰⁶ The European Union Data Protection Directive contains a similar provision.⁴⁰⁷

Why are these harms of inaccuracy understood as privacy injuries? Why does the law protect against these harms? Why should people have a right to be judged accurately?

I refer to these harms as “distortion.” Distortion is the manipulation of the way a person is perceived and judged by others, and involves the victim being inaccurately exposed to the public. ~~I include distortion in the taxonomy of privacy because of its significant similarity to other privacy disruptions.~~ Distortion, like disclosure, involves the spreading of information that affects the way society views a person. Both distortion and disclosure can result in embarrassment, humiliation, stigma, and reputational harm. They both involve the ability to control information about oneself and to have some limited dominion over the way one is viewed by society. Distortion differs from disclosure, however, because with distortion, the information revealed is false and misleading.

Throughout most of western history, one’s reputation and character have been viewed as indispensable to self-identity and the ability to engage in public life. For centuries, the loss of social regard has had deleterious effects on one’s wealth, prosperity, and employment.⁴⁰⁸ Social regard, acceptance, and honor are extremely valuable, and they have power over us because they are integral to how we relate to others. Robert Post observes that defamation law also exists for

the protection of an individual’s interest in dignity, which is to say his interest in being included within the forms of social respect; and the enforcement of

⁴⁰⁵ See U.S. DEP’T OF HEALTH, EDUC., & WELFARE, *supra* note 168, at xx-xxiii (listing and discussing “safeguard requirements” and recommendations for automated personal data systems).

⁴⁰⁶ ORG. FOR ECON. CO-OPERATION & DEV., OECD GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA (1980). For more background on the OECD Guidelines, see Joel R. Reidenberg, *Restoring Americans’ Privacy in Electronic Commerce*, 14 BERKELEY TECH. L.J. 771, 773-81 (1999).

⁴⁰⁷ Council Directive 95/46, *supra* note 46, art. 6.

⁴⁰⁸ Arlette Farge, *The Honor and Secrecy of Families*, in 3 A HISTORY OF PRIVATE LIFE 571, 585 (Roger Chartier ed., Arthur Goldhammer trans., 1989). Heinrich Böll’s novella, *The Lost Honor of Katharina Blum*, is a remarkable account of the harm of distortion. See HEINRICH BÖLL, *THE LOST HONOR OF KATHARINA BLUM* (Leila Vennewitz trans., 1975) (featuring a character whose life is ruined due to the publication of misleading information).

society's interest in its rules of civility, which is to say its interest in defining and maintaining the contours of its own social constitution.⁴⁰⁹

Reputation is not merely an individual creation. Although it is true that people work very hard to build their reputations, one's reputation is the product of the judgment of other people in society. Reputation is a currency through which we interact with each other. Protection against distortion structures our interactions because it protects this currency. Distortion not only affects the aggrieved individual; it also affects the society that judges that individual: it interferes with our relationships to that individual, and it inhibits our ability to assess the character of those that we deal with. We are thus deceived in our relationships with others; these relationships are tainted by false information that prevents us from making sound and fair judgments. Distortion's direct impact is felt by the aggrieved individual, but it has effects for all of society. We want to avoid arbitrary and undeserved disruption of social relations.

The enigmatic and devious Iago's comments in William Shakespeare's *Othello* capture the importance of reputation:

Good name in man and woman, dear my lord,
Is the immediate jewel of their souls;
Who steals my purse steals trash: 'tis something, nothing;
'Twas mine, 'tis his, and has been slave to thousands.
But he that filches from me my good name
Robs me of that which not enriches him
And makes me poor indeed.⁴¹⁰

Using the power of reputation, Iago orchestrates a series of distortions to make Othello believe that his wife, Desdemona, is having an affair with his lieutenant, Cassio. These distortions induce Othello into a murderous rage, during which he suffocates his wife. *Othello* illustrates the profound destructiveness of distortion, which tears apart relationships, dissolves trust, and instigates violence.

D. *Invasion*

The final grouping of privacy harms I label as "invasion." Invasion harms differ from the harms of information collection, networking, and dissemination because they do not always involve information. I discuss two types of invasion: (1) intrusion, and (2) decisional interference.

⁴⁰⁹ Robert C. Post, *The Social Foundations of Defamation Law: Reputation and the Constitution*, 74 CAL. L. REV. 691, 711 (1986).

⁴¹⁰ WILLIAM SHAKESPEARE, *THE TRAGEDY OF OTHELLO, THE MOOR OF VENICE* act 3, sc. 3, ll. 158-64 (Edward Pechter ed., W.W. Norton & Co. 2004) (1623).

1. Intrusion

For hundreds of years, the law has strongly guarded the privacy of the home.⁴¹¹ According to William Blackstone, "the law . . . has so particular and tender a regard to the immunity of a man's house, that it stiles it his castle."⁴¹² The law protects the home from trespass by others as well as from nuisances.⁴¹³ As Thomas Cooley observed in his famous treatise on constitutional law in 1868, "it is better oftentimes that crime should go unpunished than that the citizen should be liable to have his premises invaded, his trunks broken open, his private books, papers, and letters exposed to prying curiosity, and to the misconstructions of ignorant and suspicious persons."⁴¹⁴ The Fourth Amendment protects the home, as well as one's body and baggage, from searches by government officials.⁴¹⁵ One of the torts inspired by Warren and Brandeis's article is intrusion upon seclusion, which creates a cause of action when one intrudes "upon the solitude or seclusion of another or his private affairs or concerns" if the intrusion is "highly offensive to a reasonable person."⁴¹⁶ Why is it important to protect a safe zone, a private realm free from intrusions?

Understood broadly, these actions are all forms of "intrusion." Intrusion involves invasions or incursions into one's life. It disturbs the victim's daily activities, alters her routines, destroys her solitude, and often makes her feel uncomfortable and uneasy. Protection against intrusion involves protecting the individual from unwanted social invasions, affording people what Warren and Brandeis called "the right to be let alone."⁴¹⁷

Intrusion is related to disclosure, as disclosure is often made possible by intrusive information gathering activities. Intrusion into one's private sphere can be caused not only by physical incursion and proximity but also

⁴¹¹ The notion that the home was one's "castle" was articulated as early as 1499. See Note, *The Right to Privacy in Nineteenth Century America*, 94 HARV. L. REV. 1892, 1894 (1981) (dating the first mention to a report written in 1499); see also *Semayne's Case*, 77 Eng. Rep. 194, 195 (K.B. 1605) ("[T]he house of every one is to him as his . . . castle and fortress.").

⁴¹² 4 WILLIAM BLACKSTONE, COMMENTARIES *223.

⁴¹³ Nuisance involves "an invasion of another's interest in the private use and enjoyment of land." RESTATEMENT (SECOND) OF TORTS § 822 (1977). William Blackstone defined private nuisance as "any thing done to the hurt or annoyance of the lands, tenements, or hereditaments of another." 3 WILLIAM BLACKSTONE, COMMENTARIES *216.

⁴¹⁴ THOMAS M. COOLEY, A TREATISE ON THE CONSTITUTIONAL LIMITATIONS WHICH REST UPON THE LEGISLATIVE POWER OF THE STATES OF THE AMERICAN UNION 306 (1868).

⁴¹⁵ U.S. CONST. amend. IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated . . .").

⁴¹⁶ RESTATEMENT (SECOND) OF TORTS § 652B.

⁴¹⁷ Warren & Brandeis, *supra* note 21, at 193.

by gazes (surveillance) or questioning (interrogation). Intrusion has a certain resemblance to surveillance, in that being stared at for extended periods of time can be quite invasive and penetrating and also disturbing, frightening, and disruptive. Intrusion is also related to interrogation, as people can experience interrogation as a kind of intrusion into their affairs.

The harm caused by intrusion, however, differs from that caused by other types of disruption because intrusion interrupts one's activities through the unwanted presence or activities of another person. The case of *Galella v. Onassis* provides a good illustration of how intrusion is related yet distinct from forms of information gathering.⁴¹⁸ Galella, a paparazzo, routinely harassed Jacqueline Onassis and her children with the late President John F. Kennedy, John and Caroline. To capture pictures, Galella jumped into John's path as he was riding his bike, interrupted Caroline's tennis, and, in the words of the trial judge, "insinuated himself into the very fabric of Mrs. Onassis' life."⁴¹⁹ Galella's activities involved monitoring, akin to surveillance, yet they were also physically intrusive.

Intrusion need not involve spatial incursions: spam, junk mail, junk faxes, and telemarketing are disruptive in a similar way, as they sap people's time and attention and interrupt their activities. While many forms of intrusion are motivated by a desire to gather information or result in the revelation of information, intrusion can cause harm even if no information is involved. In particular, intrusion often interferes with solitude, the state of being alone or able to retreat from the presence of others. Indeed, Warren and Brandeis wrote from a tradition of solitude inspired by Ralph Waldo Emerson, Henry David Thoreau, and Emily Dickinson.⁴²⁰

For centuries, however, solitude has been criticized as self-indulgent.⁴²¹ As Aristotle observed: "Surely it is strange, too, to make the supremely happy man a solitary; for no one would choose the whole world on condition of being alone, since man is a political creature and one whose nature is

telco
calls

⁴¹⁸ 487 F.2d 986 (2d Cir. 1973).

⁴¹⁹ *Id.* at 994 (quoting *Galella v. Onassis*, 353 F. Supp. 196, 228 (S.D.N.Y. 1972)).

⁴²⁰ Dorothy J. Glancy, *The Invention of the Right to Privacy*, 21 ARIZ. L. REV. 1, 25 (1979).

⁴²¹ See, e.g., JANETTE DILLON, *SHAKESPEARE AND THE SOLITARY MAN* 3-13 (1981) (discussing approaches to solitude before Shakespeare's time, which viewed a solitary life as running counter to the good of the community). Solitude, which became a coveted aspect of existence by the end of the seventeenth century, was viewed by many as dangerous and undesirable during the Middle Ages. See Michel Rouché, *Private Life Conquers State and Society*, in 1 A HISTORY OF PRIVATE LIFE, *supra* note 408, at 419, 434-35 (describing the concern a ninth-century abbot had for the hermit's solitary life).

to live with others."⁴²² Under this view, solitude is a form of retreat from solidarity, a condition of being isolated and self-interested in which a person can escape her social responsibilities.⁴²³ Too much of such freedom from intrusion can lead to a scattered community, where people distance themselves into isolated enclaves.⁴²⁴ Why do we want to allow people to have a realm in which they can avoid the presence of others in society?

The protection of a realm of solitude does not merely benefit the individual; it is built into society's structure for a social purpose. Hannah Arendt notes that while the Greeks viewed the public sphere as having paramount importance, the private sphere was essential to shaping the dimensions and quality of life in the public sphere:

A life spent entirely in public, in the presence of others, becomes, as we would say, shallow. While it retains its visibility, it loses the quality of rising into sight from some darker ground which must remain hidden if it is not to lose its depth in a very real, non-subjective sense.⁴²⁵

In other words, solitude does not detract from a rich public life, but in fact enhances it. Solitude enables people to rest from the pressures of living in public and performing public roles.⁴²⁶ Too much envelopment in society can be destructive to social relationships. For Thoreau, solitude fosters better social relationships because "we live thick and are in each other's way, and stumble over one another, and I think that we thus lose some respect for one another."⁴²⁷ Without refuge from others, relationships can become more bitter and tense. Moreover, a space apart from others has enabled people to develop artistic, political, and religious ideas that have had lasting influence and value when later introduced into the public sphere.⁴²⁸

⁴²² ARISTOTLE, *ETHICA NICOMACHEA* § 1169b, ll. 18-19 (W.D. Ross trans., Clarendon Press 1925) (n.d.).

⁴²³ See Michael A. Weinstein, *The Uses of Privacy in the Good Life*, in NOMOS, *supra* note 71, at 88, 91-93 (discussing critiques of solitude).

⁴²⁴ See LEWIS MUMFORD, *THE CITY IN HISTORY* 512-13 (1961) (demonstrating how technological improvements have led to increased isolation).

⁴²⁵ HANNAH ARENDT, *THE HUMAN CONDITION* 71 (1958).

⁴²⁶ According to philosopher Philip Koch, solitude "gives respite and restoration, a time and a place to lick the wounds of social strife." PHILIP KOCH, *SOLITUDE* 5 (1994); see also WESTIN, *supra* note 19, at 35 ("[N]o individual can play indefinitely, without relief, the variety of roles that life demands. . . . Privacy in this aspect gives individuals, from factory workers to Presidents, a chance to lay their masks aside for rest. To be always 'on' would destroy the human organism.").

⁴²⁷ HENRY DAVID THOREAU, *Walden*, in *WALDEN AND OTHER WRITINGS* 113 (Barnes & Noble Books 1993) (1854).

⁴²⁸ Many social, political, and religious leaders began their influential public work with preparations performed in private. See, e.g., JOSEPH BENSMAN & ROBERT LILIENFELD, *BETWEEN PUBLIC AND PRIVATE: THE LOST BOUNDARIES OF THE SELF* 37 (1979) (describing

Generally, courts recognize intrusion upon seclusion tort actions only when a person is at home or in a secluded place.⁴²⁹ This approach is akin to courts recognizing a harm in surveillance only when conducted in private, not in public.⁴³⁰ However, beyond solitude, people often expect space from others—even when they are with other people. According to sociologist Irwin Altman, we need “personal space,” a kind of zone or aura around us to separate ourselves from others.⁴³¹ Spatial distance provides for “comfort, ease, and relaxation.”⁴³² Animals maintain “remarkably constant” distances from other animals of the same species.⁴³³ In one series of studies, people placed themselves very close to others, sparking strong reactions of hostility and unease; the intruded-upon subjects quickly reestablished appropriate spatial boundaries.⁴³⁴ As Robert Post observes, the tort of intrusion upon seclusion upholds rules of civility and social respect.⁴³⁵ We each have certain “territories of the self,” and norms of civility require that we respect others’ territories.⁴³⁶ We can, however, “invite intimacy by waiving our claims to a territory and allowing others to draw close.”⁴³⁷

Some courts are beginning to recognize realms of exclusion where people can shut others out, even in public.⁴³⁸ Realms of *exclusion* are not

how a “religious hero[’s]” retreat to privacy would inspire followers on his return to the public life); Richard H. Weisberg, *It’s a Positivist, It’s a Pragmatist, It’s a Codifier! Reflections on Nietzsche and Stendhal*, 18 CARDOZO L. REV. 85, 92 (1996) (noting that, for Nietzsche, “[t]he great legislator is himself (or herself) conceived of as one whose act of social codification begins with a private program of creative self-fulfillment”). As sixteenth-century French essayist Michel de Montaigne contended, solitude—even for public figures—is not self-indulgent, for “[t]hey have only stepped back to make a better jump, to get a stronger impetus wherewith to plunge deeper into the crowd.” MICHEL DE MONTAIGNE, *Of Solitude*, in THE COMPLETE ESSAYS OF MONTAIGNE 174, 182 (Donald M. Frame trans., 1958).

⁴²⁹ See, e.g., RESTATEMENT (SECOND) OF TORTS § 652B cmt. c (1977) (“The defendant is subject to liability . . . only when he has intruded into a private place, or has otherwise invaded a private seclusion that the plaintiff has thrown about his person or affairs.”).

⁴³⁰ See *supra* notes 81-104 and accompanying text.

⁴³¹ IRWIN ALTMAN, THE ENVIRONMENT AND SOCIAL BEHAVIOR: PRIVACY, PERSONAL SPACE, TERRITORY, CROWDING 52-54 (Irvington 1981) (1975).

⁴³² *Id.* at 96.

⁴³³ *Id.* at 52.

⁴³⁴ *Id.* at 87-89.

⁴³⁵ Post, *supra* note 44, at 966-68.

⁴³⁶ *Id.* at 971-73 (citing Erving Goffman, *The Territories of the Self*, in RELATIONS IN PUBLIC 28 (1971)).

⁴³⁷ *Id.* at 973.

⁴³⁸ See, e.g., *Shulman v. Group W Prods., Inc.*, 955 P.2d 469, 491 (Cal. 1998) (holding that a car accident victim had a privacy interest in her conversation with medical rescuers at the accident scene); *Stressman v. Am. Black Hawk Broad. Co.*, 416 N.W.2d 685, 687-88 (Iowa 1987) (holding that broadcasting video of the plaintiff eating at a restaurant might have violated her privacy interest and noting that “the mere fact a person can be seen by others does

realms of *seclusion*; they are structures for personal space that allow us to interact with others without the interference of the rest of society. Communication and association with others often require freedom from intrusion. For example, when we talk to a friend in a restaurant or another public place, we still need space from other people in order to converse freely. In *Sanders v. American Broadcasting Companies*, an undercover reporter accepted work as a "telepsychic" and surreptitiously videotaped conversations she had at work with her coworkers, including Sanders.⁴³⁹ Even though Sanders worked in a cubicle where he could readily be seen and overheard by other employees, the court concluded that he had a viable privacy interest: "[T]he concept of 'seclusion' is relative. The mere fact that a person can be seen by someone does not automatically mean that he or she can legally be forced to be subject to being seen by everyone."⁴⁴⁰

2. Decisional Interference

In 1965, in *Griswold v. Connecticut*, the Supreme Court held that the Constitution prohibited the government from banning the use of contraceptives by married couples.⁴⁴¹ Although the word "privacy" is not explicitly mentioned anywhere in the Constitution, the Court reasoned that the Constitution provides for a "right to privacy" in the "penumbras" of many of the amendments in the Bill of Rights.⁴⁴² The Court noted that "[v]arious guarantees [by the Bill of Rights] create zones of privacy."⁴⁴³

In *Eisenstadt v. Baird*, the Court extended the reasoning in *Griswold* to the use of contraceptives by unmarried persons as well.⁴⁴⁴ The Court explained that privacy "is the right of the individual, married or single, to be free from unwarranted governmental intrusion into matters so fundamentally affecting a person as the decision whether to bear or beget a child."⁴⁴⁵ Subsequently, the Court held in *Roe v. Wade* that the right to privacy "encompass[es] a woman's decision whether or not to terminate her pregnancy."⁴⁴⁶

not mean that person cannot legally be 'secluded'"(quoting *Huskey v. Nat'l Broad. Co.*, 632 F. Supp. 1282, 1287-88 (N.D. Ill. 1986)).

⁴³⁹ 978 P.2d 67, 69-70 (Cal. 1999).

⁴⁴⁰ *Id.* at 72 (quoting 1 MCCARTHY, *supra* note 3, § 5.10[A][2]).

⁴⁴¹ 381 U.S. 479, 485-86 (1965).

⁴⁴² *Id.* at 484.

⁴⁴³ *Id.*

⁴⁴⁴ 405 U.S. 438 (1972).

⁴⁴⁵ *Id.* at 453 (emphasis omitted).

⁴⁴⁶ 410 U.S. 113, 153 (1973).

Griswold, *Eisenstadt*, and *Baird* all protect against what I call "decisional interference"—that is, governmental interference with people's decisions regarding certain matters of their lives. These cases extend to decisions relating to sex and sexuality, while others extend to decisions concerning the upbringing of one's children.⁴⁴⁷ Many commentators have argued that the language of privacy is inappropriate for decisional interference cases, since they primarily concern a harm to autonomy and liberty, not to privacy. Thus, Laurence Tribe argues that the central issue in *Roe v. Wade* is "not privacy, but autonomy."⁴⁴⁸ Similarly, Louis Henkin contends that the Supreme Court's substantive due process right-to-privacy cases are about protecting a "zone of autonomy, of presumptive immunity to governmental regulation," not about protecting privacy.⁴⁴⁹ What relationship does decisional interference have with the other forms of privacy in the taxonomy?

The decisional interference cases are deeply connected to information privacy.⁴⁵⁰ In particular, just a few years after *Roe v. Wade*, the Court explained in *Whalen v. Roe* that the constitutionally protected "zone of privacy" extends not only to the "interest in independence in making certain kinds of important decisions" but also to the "individual interest in avoiding disclosure of personal matters."⁴⁵¹ This gave rise to the constitutional right to information privacy, which, although not developed further by the Supreme Court, has been recognized by most federal circuit courts.⁴⁵² *Whalen*

⁴⁴⁷ See, e.g., *Pierce v. Soc'y of Sisters*, 268 U.S. 510, 534-35 (1925) (invalidating an Oregon law requiring parents to send their children to public school, because it "unreasonably interfere[d] with the liberty of parents . . . to direct the upbringing and education of children under their control").

⁴⁴⁸ LAURENCE H. TRIBE, *AMERICAN CONSTITUTIONAL LAW* 1352 (2d ed. 1988).

⁴⁴⁹ Louis Henkin, *Privacy and Autonomy*, 74 COLUM. L. REV. 1410, 1410-11 (1974).

⁴⁵⁰ Thanks to Neil Richards for pointing this out.

⁴⁵¹ 429 U.S. 589, 599-600 (1977).

⁴⁵² See, e.g., *In re Crawford*, 194 F.3d 954, 958 (9th Cir. 1999) ("We agree . . . that the indiscriminate public disclosure of [certain personal information] may implicate the constitutional right to informational privacy."); *Walls v. City of Petersburg*, 895 F.2d 188, 192 (4th Cir. 1990) ("Personal, private information in which an individual has a reasonable expectation of confidentiality is protected by one's constitutional right to privacy."); *Kimberlin v. U.S. Dep't of Justice*, 788 F.2d 434, 438 (7th Cir. 1986) ("Whether or not Kimberlin has a privacy interest in the information . . . depends upon whether he has a reasonable expectation of privacy in the information."); *Barry v. City of New York*, 712 F.2d 1554, 1559 (2d Cir. 1983) ("Most courts considering the question . . . appear to agree that privacy of personal matters is a [constitutionally] protected interest . . ."); *J.P. v. DeSanti*, 653 F.2d 1080, 1090 (6th Cir. 1981) ("Our opinion does not mean . . . there is no constitutional right to non-disclosure of private information."); *United States v. Westinghouse Elec. Corp.*, 638 F.2d 570, 577 (3d Cir. 1980) (recognizing that *Whalen* protects "the right not to have an individual's private affairs made public by the government"); *Plante v. Gonzalez*, 575 F.2d 1119, 1132 (5th Cir. 1978) ("There is another strand to the right to privacy properly called the right to confidentiality.").

involved a challenge to a requirement that physicians report to the state the names and addresses of patients who received prescriptions for certain classes of drugs. The *Whalen* Court linked decisional interference with disclosure by suggesting that “[t]he mere existence in readily available form of the information about patients’ use of [the] drugs creates a genuine concern that the information will become publicly known and that it will adversely affect their reputations. This concern makes some patients reluctant to use [the drugs]”⁴⁵³ By creating a risk of disclosure, the statute inhibited patients’ decisions regarding their healthcare.⁴⁵⁴ The Court ultimately rejected the plaintiff’s challenge because the state provided adequate protection against the “unwarranted disclosure” of the patient information.⁴⁵⁵ Thus, *Whalen* illustrates how decisional interference relates to disclosure. *Whalen* also shows how decisional interference bears similarities to increased accessibility, since the existence of information in a government database can increase the potential accessibility of that information.

Decisional interference also resembles insecurity, secondary use, and exclusion, in that all three of these information-processing harms can have a chilling effect on a person’s decisions regarding her health and body.

Decisional interference and exposure have been judicially recognized to affect the same aspects of the self—health, the body, sex, and so on. The decisional interference cases track traditional areas that are widely considered to be private, such as the home, family, and body. Decisional interference, therefore, does not apply to all decisions, but only to a subset of decisions; this aspect of decisional interference resembles exposure in its focus on those aspects of life which are socially considered to be the most private.

Decisional interference bears a similarity to the harm of intrusion as both involve invasions into realms where we believe people should be free from the incursions of others. Whereas intrusion involves the unwanted general incursion of another’s presence or activities, decisional interference involves unwanted incursion *by the government* into an individual’s *decisions* about her personal life. The resemblance is demonstrated by examining the first in the Court’s line of right-to-privacy cases, its 1891 decision in *Union Pacific Railway Co. v. Botsford*.⁴⁵⁶ There, the Court held that a female plaintiff in a civil action could not be forced to submit to a surgical examination: “To compel any one, and especially a woman, to lay bare the body, or to submit it to the touch of a stranger, without lawful authority, is

⁴⁵³ *Whalen*, 429 U.S. at 600.

⁴⁵⁴ *Id.*

⁴⁵⁵ *Id.* at 600-02.

⁴⁵⁶ 141 U.S. 250 (1891).

an indignity, an assault, and a trespass. . . ."⁴⁵⁷ The Court emphasized the importance of what Judge Cooley had termed the right "to be let alone" which Warren and Brandeis used in their article one year earlier.⁴⁵⁸ While the intrusion at issue in *Botsford* clearly implicated the harms of intrusion and exposure, it also resembled decisional interference. The Court captured this parallel in stating that the right "to be let alone" was "carefully guarded by the common law" and consisted of "the right of every individual to the possession and control of his own person, free from all restraint or interference of others, unless by clear and unquestionable authority of law."⁴⁵⁹

Another case illustrating the connection between decisional interference and intrusion is *Stanley v. Georgia*, which involved a challenge to an obscenity statute that punished the private possession of obscene material.⁴⁶⁰ *Stanley* was cited as support for the constitutional right to privacy in *Roe v. Wade*⁴⁶¹ and *Eisenstadt v. Baird*.⁴⁶² Although the material in *Stanley* was obscene and could properly be banned under the First Amendment, the Court concluded that "the Constitution protects the right to receive information and ideas . . . regardless of their social worth."⁴⁶³ The Court noted that this "right takes on an added dimension" in a "prosecution for mere possession of printed or filmed matter in the privacy of a person's own home."⁴⁶⁴ It is a fundamental right "to be free, except in very limited circumstances, from unwanted governmental intrusions into one's privacy."⁴⁶⁵ The Court quoted Justice Brandeis's dissent in *Olmstead v. United States*,⁴⁶⁶ a Fourth Amendment wiretapping case, in which Brandeis argued that the "makers of our Constitution . . . conferred, as against the Government, the right to be let alone—the most comprehensive of rights and the right most valued by civilized man."⁴⁶⁷

It is particularly interesting that the Court invoked "the right to be let alone," which was Warren and Brandeis's principle justifying the privacy torts.⁴⁶⁸ The criminalization of the private possession of obscene material,

⁴⁵⁷ *Id.* at 252.

⁴⁵⁸ *Id.* at 251; Warren & Brandeis, *supra* note 21, at 195.

⁴⁵⁹ *Union Pacific*, 141 U.S. at 251.

⁴⁶⁰ 394 U.S. 557 (1969).

⁴⁶¹ 410 U.S. 113, 152 (1973).

⁴⁶² 405 U.S. 438, 453 (1972).

⁴⁶³ *Stanley*, 394 U.S. at 564.

⁴⁶⁴ *Id.*

⁴⁶⁵ *Id.*

⁴⁶⁶ 277 U.S. 438 (1928).

⁴⁶⁷ *Stanley*, 395 U.S. at 564 (quoting *Olmstead*, 277 U.S. at 478 (Brandeis, J., dissenting) (internal quotation marks omitted)).

⁴⁶⁸ See Warren & Brandeis, *supra* note 21, at 195.

the Court's reasoning suggests, necessitates governmental intrusion into one's home. The Court noted that people have "the right to be free from state inquiry into the contents of [their] library."⁴⁶⁹ Linking decisional interference with intrusion, it stressed that "a State has no business telling a man, sitting alone in his own house, what books he may read or what films he may watch."⁴⁷⁰ Further capturing the relationship between the two categories, Robert Post contends that the intrusion tort protects "territories of the self," which are critical to remaining "an independent and autonomous person."⁴⁷¹

In *Lawrence v. Texas*, the Court further demonstrated the frequent overlap between decisional interference and intrusion in striking down a law that prohibited consensual homosexual sodomy.⁴⁷² The Court reasoned that "adults may choose to enter upon this relationship in the confines of their homes and their own private lives and still retain their dignity as free persons."⁴⁷³ The statute was unconstitutional because of "its [unjustified] intrusion into the personal and private life of the individual."⁴⁷⁴ Moreover, the Court stated:

Liberty protects the person from unwarranted government intrusions into a dwelling or other private places. In our tradition the State is not omnipresent in the home. And there are other spheres of our lives and existence, outside the home, where the State should not be a dominant presence. Freedom extends beyond spatial bounds.⁴⁷⁵

The Court thus linked decisional interference to intrusion.

Decisional interference also bears an indirect resemblance to blackmail, in that laws restricting consensual private sexual behavior often give rise to blackmail. The *Lawrence* Court noted that in 1955, when crafting the Model Penal Code, the American Law Institute recommended against criminalizing "consensual sexual relations conducted in private"⁴⁷⁶ in part because "the statutes regulated private conduct not harmful to others," and because "the laws were arbitrarily enforced and thus invited the danger of blackmail."⁴⁷⁷ Indeed, as Angus McLaren recounts, blackmail historically

⁴⁶⁹ *Stanley*, 395 U.S. at 565.

⁴⁷⁰ *Id.*

⁴⁷¹ Post, *supra* note 44, at 973.

⁴⁷² 539 U.S. 558, 578 (2003).

⁴⁷³ *Id.* at 567.

⁴⁷⁴ *Id.* at 578.

⁴⁷⁵ *Id.* at 562.

⁴⁷⁶ *Id.* at 572 (quoting MODEL PENAL CODE § 213.2 cmt. 2 (1980)).

⁴⁷⁷ *Id.* (citing MODEL PENAL CODE § 207.5 cmt. at 277-78 (Tentative Draft No. 4, 1955)). For an interesting discussion of *Lawrence* and public versus private places, see Lior

occurred in the shadow of laws that punished consensual sexual activities in private.⁴⁷⁸ McLaren writes: "Society preferred to blame the eruption of blackmail on certain 'dangerous' women and men rather than come to terms with the tension between the laws and the sexual practices that often provided temptation to unscrupulous individuals."⁴⁷⁹

CONCLUSION

In 1960, William Prosser identified ~~just~~ four interests under the rubric of privacy, and focused exclusively on tort law. His effort is far too narrow and far too out-of-date to serve as an effective guide to the privacy problems we face today. In this Article, I have attempted to provide a clearer and more robust account of privacy—one that provides us with a framework for understanding privacy problems. The taxonomy demonstrates that privacy disruptions are different from one another and yet share important similarities. The taxonomy enables us to see privacy in a more multidimensional way.⁴⁸⁰

Although all of the privacy harms I identify in the taxonomy are related in some way, they are not all related in the same way—there is no common denominator that links them all. Privacy violations are a group of related harms, each of which has received at least some recognition in the law. But our understanding of privacy remains in a fog, and the law remains fragmented and inconsistent.

Too many courts and policymakers struggle with even identifying the presence of a privacy problem. Protecting privacy requires careful balancing, as neither privacy nor its countervailing interests are absolute values. Unfortunately, due to conceptual confusion, courts and legislatures often fail to recognize privacy problems, and thus no balancing ever takes place. This does not mean that privacy should always win in the balance, but it should not be dismissed just because it is ignored or misconstrued.

Jacob Strahilevitz, *Consent, Aesthetics, and the Boundaries of Sexual Privacy After Lawrence v. Texas*, 54 DEPAUL L. REV. 671 (2005).

⁴⁷⁸ MCLAREN, *supra* note 353, at 6.

⁴⁷⁹ *Id.* at 8.

⁴⁸⁰ One might ask why we should even retain the term "privacy" if it is simply a broader way to describe a group of different types of harms. Why not simply refer to the particular harms themselves and jettison the term "privacy" altogether? But this view overlooks a key aspect of the way we refer to things and think about them. Although the various harms I identify in the taxonomy are different from one another, and although they do not have a core characteristic in common, they do, as I have shown in this Article, share many important similarities.

When translated into the legal system, privacy is a form of protection against certain harmful or problematic activities. The activities that affect privacy are not necessarily socially undesirable or worthy of sanction or prohibition. This fact is what makes addressing privacy issues so complex. In many instances, there is no clear-cut wrongdoer, no indisputable villain whose activities lack social value. Instead, many privacy problems emerge as a result of efficacious activities, much like pollution is an outgrowth of industrial production. With the taxonomy, I have attempted to demonstrate that these activities are not without cost, that they have certain nontrivial effects on people's lives and well-being.

Courts and policymakers often have great difficulty in arriving at a coherent assessment of the various privacy problems and harms that they must address. One common pitfall is viewing "privacy" as a particular kind of harm to the exclusion of all others. As illustrated throughout this Article, courts generally find no privacy interest if information is in the public domain, if people are monitored in public, if information is gathered in a public place, if no intimate or embarrassing details are revealed, or if no new data is collected about a person. If courts and legislatures focused instead on the privacy *problems*, many of these distinctions and determinative factors would matter much less in the analysis. Thus, when analyzing surveillance issues, courts focus on whether the surveillance occurs in public or in private, even though problems and harms can emerge in all settings. Aggregation creates problems even when all of the data is already available in the public domain. The same is true of increased accessibility. For disclosure, the secrecy of the information becomes a central dispositive factor; this approach often misses the crux of the disclosure harm, which is not the revelation of total secrets, but the spreading of information beyond expected boundaries. In intrusion analyses, courts often fail to recognize harm when people are intruded upon in public places, yet the nature of the harm is not limited solely to private places.

At other times, the privacy problem at issue is misconstrued. For example, identification is often understood as a harm created by revealing one's name, but the essence of the problem is being linked to a stream of data, not only a name. Insecurity is often not adequately addressed by the law because a materialized harm has not yet occurred. But insecurity remains a problem, even where there has been no actual disclosure or leakage of embarrassing details. Appropriation is understood primarily as a harm to property interests, and its dignitary dimensions are thus frequently ignored by courts. Further complicating matters is the fact that privacy problems are inconsistently recognized across different areas of the law. For example,

tort law readily recognizes and redresses breach of confidentiality, yet Fourth Amendment law ignores it as a harm.

Courts and legislatures respond well to more traditional privacy problems, such as intrusions that are physical in nature, disclosures of deep secrets, or distortion. This is due, in part, to the fact that these problems track traditional conceptions of privacy. In the secrecy paradigm, a privacy violation is understood as the uncovering of a person's hidden world. Physical intrusions are problems that even people in ancient times could experience and understand. But some of the privacy problems we face today are different in nature, and do not track traditional conceptions of privacy. They involve efforts to gain knowledge about an individual without physically intruding or even gathering data directly from them (aggregation), or problems that emerge from the way that the data is handled and maintained (insecurity), the way it is used (secondary use), and the inability of people to participate in its processing (exclusion). Modern privacy problems emerge not just from disclosing deep secrets, but from making obscure information more accessible (increased accessibility) or from consistent observation or eavesdropping (surveillance).

The taxonomy lays down a framework to understand the range of privacy problems, the similarities and differences among them, the relationships among them, and what it is that makes them problematic. By focusing on *activities*, the taxonomy also seeks to emphasize how privacy problems arise. Often, technology is involved in various privacy problems, as it facilitates the gathering, processing, and dissemination of information. Privacy problems, however, are caused not by technology alone, but primarily through *activities* of people, businesses, and the government. The way to address privacy problems is to regulate these activities.

With a framework for identifying and understanding privacy problems, courts and policymakers can better balance privacy considerations against countervailing interests. This Article is thus the beginning of what will hopefully be a more comprehensive and coherent understanding of privacy.

Read 11/3

TITLE 15 - COMMERCE AND TRADE

CHAPTER 2 - FEDERAL TRADE COMMISSION; PROMOTION OF EXPORT TRADE AND PREVENTION OF UNFAIR METHODS OF COMPETITION

SUBCHAPTER I - FEDERAL TRADE COMMISSION

FTC

§ 45. Unfair methods of competition unlawful; prevention by Commission

(a) **Declaration of unlawfulness; power to prohibit unfair practices; inapplicability to foreign trade**

(1) Unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful.

(2) The Commission is hereby empowered and directed to prevent persons, partnerships, or corporations, except banks, savings and loan institutions described in section 57a (f)(3) of this title, Federal credit unions described in section 57a (f)(4) of this title, common carriers subject to the Acts to regulate commerce, air carriers and foreign air carriers subject to part A of subtitle VII of title 49, and persons, partnerships, or corporations insofar as they are subject to the Packers and Stockyards Act, 1921, as amended [7 U.S.C. 181 et seq.], except as provided in section 406(b) of said Act [7 U.S.C. 227 (b)], from using unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce.

(3) This subsection shall not apply to unfair methods of competition involving commerce with foreign nations (other than import commerce) unless—

(A) such methods of competition have a direct, substantial, and reasonably foreseeable effect—

(i) on commerce which is not commerce with foreign nations, or on import commerce with foreign nations; or

(ii) on export commerce with foreign nations, of a person engaged in such commerce in the United States; and

(B) such effect gives rise to a claim under the provisions of this subsection, other than this paragraph.

If this subsection applies to such methods of competition only because of the operation of subparagraph (A)(ii), this subsection shall apply to such conduct only for injury to export business in the United States.

(4) (A) For purposes of subsection (a), the term “unfair or deceptive acts or practices” includes such acts or practices involving foreign commerce that—

(i) cause or are likely to cause reasonably foreseeable injury within the United States; or

(ii) involve material conduct occurring within the United States.

(B) All remedies available to the Commission with respect to unfair and deceptive acts or practices shall be available for acts and practices described in this paragraph, including restitution to domestic or foreign victims.

(b) **Proceeding by Commission; modifying and setting aside orders**

Whenever the Commission shall have reason to believe that any such person, partnership, or corporation has been or is using any unfair method of competition or unfair or deceptive act or practice in or affecting commerce, and if it shall appear to the Commission that a proceeding by it in respect thereof would be to the interest of the public, it shall issue and serve upon such person, partnership, or corporation a complaint stating its charges in that respect and containing a notice of a hearing upon a day and at a place therein fixed at least thirty days after the service of said complaint. The person, partnership, or corporation so complained of shall have the right to appear at the place and time so fixed and show cause why an order should not be entered by the Commission requiring such person, partnership, or corporation to cease and desist from the violation of the law so charged in said complaint. Any person,

partnership, or corporation may make application, and upon good cause shown may be allowed by the Commission to intervene and appear in said proceeding by counsel or in person. The testimony in any such proceeding shall be reduced to writing and filed in the office of the Commission. If upon such hearing the Commission shall be of the opinion that the method of competition or the act or practice in question is prohibited by this subchapter, it shall make a report in writing in which it shall state its findings as to the facts and shall issue and cause to be served on such person, partnership, or corporation an order requiring such person, partnership, or corporation to cease and desist from using such method of competition or such act or practice. Until the expiration of the time allowed for filing a petition for review, if no such petition has been duly filed within such time, or, if a petition for review has been filed within such time then until the record in the proceeding has been filed in a court of appeals of the United States, as hereinafter provided, the Commission may at any time, upon such notice and in such manner as it shall deem proper, modify or set aside, in whole or in part, any report or any order made or issued by it under this section. After the expiration of the time allowed for filing a petition for review, if no such petition has been duly filed within such time, the Commission may at any time, after notice and opportunity for hearing, reopen and alter, modify, or set aside, in whole or in part any report or order made or issued by it under this section, whenever in the opinion of the Commission conditions of fact or of law have so changed as to require such action or if the public interest shall so require, except that

- (1) the said person, partnership, or corporation may, within sixty days after service upon him or it of said report or order entered after such a reopening, obtain a review thereof in the appropriate court of appeals of the United States, in the manner provided in subsection (c) of this section; and
- (2) in the case of an order, the Commission shall reopen any such order to consider whether such order (including any affirmative relief provision contained in such order) should be altered, modified, or set aside, in whole or in part, if the person, partnership, or corporation involved files a request with the Commission which makes a satisfactory showing that changed conditions of law or fact require such order to be altered, modified, or set aside, in whole or in part. The Commission shall determine whether to alter, modify, or set aside any order of the Commission in response to a request made by a person, partnership, or corporation under paragraph ¹ (2) not later than 120 days after the date of the filing of such request.

(c) Review of order; rehearing

Any person, partnership, or corporation required by an order of the Commission to cease and desist from using any method of competition or act or practice may obtain a review of such order in the court of appeals of the United States, within any circuit where the method of competition or the act or practice in question was used or where such person, partnership, or corporation resides or carries on business, by filing in the court, within sixty days from the date of the service of such order, a written petition praying that the order of the Commission be set aside. A copy of such petition shall be forthwith transmitted by the clerk of the court to the Commission, and thereupon the Commission shall file in the court the record in the proceeding, as provided in section 2112 of title 28. Upon such filing of the petition the court shall have jurisdiction of the proceeding and of the question determined therein concurrently with the Commission until the filing of the record and shall have power to make and enter a decree affirming, modifying, or setting aside the order of the Commission, and enforcing the same to the extent that such order is affirmed and to issue such writs as are ancillary to its jurisdiction or are necessary in its judgement to prevent injury to the public or to competitors pendente lite. The findings of the Commission as to the facts, if supported by evidence, shall be conclusive. To the extent that the order of the Commission is affirmed, the court shall thereupon issue its own order commanding obedience to the terms of such order of the Commission. If either party shall apply to the court for leave to adduce additional evidence, and shall show to the satisfaction of the court that such additional evidence is material and that there were reasonable grounds for the failure to adduce such evidence in the proceeding before the Commission, the court may order such additional evidence to be taken before the Commission and to be adduced upon the hearing in such manner and upon such terms and conditions as to the court may seem proper. The Commission may modify its findings as to the facts,

NB: This unofficial compilation of the U.S. Code is current as of Jan. 4, 2012 (see <http://www.law.cornell.edu/uscode/uscpri.html>).

or make new findings, by reason of the additional evidence so taken, and it shall file such modified or new findings, which, if supported by evidence, shall be conclusive, and its recommendation, if any, for the modification or setting aside of its original order, with the return of such additional evidence. The judgment and decree of the court shall be final, except that the same shall be subject to review by the Supreme Court upon certiorari, as provided in section 1254 of title 28.

(d) Jurisdiction of court

Upon the filing of the record with it the jurisdiction of the court of appeals of the United States to affirm, enforce, modify, or set aside orders of the Commission shall be exclusive.

(e) Exemption from liability

No order of the Commission or judgement of court to enforce the same shall in anywise relieve or absolve any person, partnership, or corporation from any liability under the Antitrust Acts.

(f) Service of complaints, orders and other processes; return

Complaints, orders, and other processes of the Commission under this section may be served by anyone duly authorized by the Commission, either

(a) by delivering a copy thereof to the person to be served, or to a member of the partnership to be served, or the president, secretary, or other executive officer or a director of the corporation to be served; or

(b) by leaving a copy thereof at the residence or the principal office or place of business of such person, partnership, or corporation; or

(c) by mailing a copy thereof by registered mail or by certified mail addressed to such person, partnership, or corporation at his or its residence or principal office or place of business. The verified return by the person so serving said complaint, order, or other process setting forth the manner of said service shall be proof of the same, and the return post office receipt for said complaint, order, or other process mailed by registered mail or by certified mail as aforesaid shall be proof of the service of the same.

(g) Finality of order

An order of the Commission to cease and desist shall become final—

(1) Upon the expiration of the time allowed for filing a petition for review, if no such petition has been duly filed within such time; but the Commission may thereafter modify or set aside its order to the extent provided in the last sentence of subsection (b).

(2) Except as to any order provision subject to paragraph (4), upon the sixtieth day after such order is served, if a petition for review has been duly filed; except that any such order may be stayed, in whole or in part and subject to such conditions as may be appropriate, by—

(A) the Commission;

(B) an appropriate court of appeals of the United States, if

(i) a petition for review of such order is pending in such court, and

(ii) an application for such a stay was previously submitted to the Commission and the Commission, within the 30-day period beginning on the date the application was received by the Commission, either denied the application or did not grant or deny the application; or

(C) the Supreme Court, if an applicable petition for certiorari is pending.

(3) For purposes of subsection (m)(1)(B) of this section and of section 57b (a)(2) of this title, if a petition for review of the order of the Commission has been filed—

(A) upon the expiration of the time allowed for filing a petition for certiorari, if the order of the Commission has been affirmed or the petition for review has been dismissed by the court of appeals and no petition for certiorari has been duly filed;

NB: This unofficial compilation of the U.S. Code is current as of Jan. 4, 2012 (see <http://www.law.cornell.edu/uscode/uscpri.html>).

- (B) upon the denial of a petition for certiorari, if the order of the Commission has been affirmed or the petition for review has been dismissed by the court of appeals; or
 - (C) upon the expiration of 30 days from the date of issuance of a mandate of the Supreme Court directing that the order of the Commission be affirmed or the petition for review be dismissed.
- (4) In the case of an order provision requiring a person, partnership, or corporation to divest itself of stock, other share capital, or assets, if a petition for review of such order of the Commission has been filed—
- (A) upon the expiration of the time allowed for filing a petition for certiorari, if the order of the Commission has been affirmed or the petition for review has been dismissed by the court of appeals and no petition for certiorari has been duly filed;
 - (B) upon the denial of a petition for certiorari, if the order of the Commission has been affirmed or the petition for review has been dismissed by the court of appeals; or
 - (C) upon the expiration of 30 days from the date of issuance of a mandate of the Supreme Court directing that the order of the Commission be affirmed or the petition for review be dismissed.

(h) Modification or setting aside of order by Supreme Court

If the Supreme Court directs that the order of the Commission be modified or set aside, the order of the Commission rendered in accordance with the mandate of the Supreme Court shall become final upon the expiration of thirty days from the time it was rendered, unless within such thirty days either party has instituted proceedings to have such order corrected to accord with the mandate, in which event the order of the Commission shall become final when so corrected.

(i) Modification or setting aside of order by Court of Appeals

If the order of the Commission is modified or set aside by the court of appeals, and if

- (1) the time allowed for filing a petition for certiorari has expired and no such petition has been duly filed, or
- (2) the petition for certiorari has been denied, or
- (3) the decision of the court has been affirmed by the Supreme Court, then the order of the Commission rendered in accordance with the mandate of the court of appeals shall become final on the expiration of thirty days from the time such order of the Commission was rendered, unless within such thirty days either party has instituted proceedings to have such order corrected so that it will accord with the mandate, in which event the order of the Commission shall become final when so corrected.

(j) Rehearing upon order or remand

If the Supreme Court orders a rehearing; or if the case is remanded by the court of appeals to the Commission for a rehearing, and if

- (1) the time allowed for filing a petition for certiorari has expired, and no such petition has been duly filed, or
- (2) the petition for certiorari has been denied, or
- (3) the decision of the court has been affirmed by the Supreme Court, then the order of the Commission rendered upon such rehearing shall become final in the same manner as though no prior order of the Commission had been rendered.

(k) "Mandate" defined

As used in this section the term "mandate", in case a mandate has been recalled prior to the expiration of thirty days from the date of issuance thereof, means the final mandate.

(l) Penalty for violation of order; injunctions and other appropriate equitable relief

NB: This unofficial compilation of the U.S. Code is current as of Jan. 4, 2012 (see <http://www.law.cornell.edu/uscode/uscodeprint.html>).

Any person, partnership, or corporation who violates an order of the Commission after it has become final, and while such order is in effect, shall forfeit and pay to the United States a civil penalty of not more than \$10,000 for each violation, which shall accrue to the United States and may be recovered in a civil action brought by the Attorney General of the United States. Each separate violation of such an order shall be a separate offense, except that in a case of a violation through continuing failure to obey or neglect to obey a final order of the Commission, each day of continuance of such failure or neglect shall be deemed a separate offense. In such actions, the United States district courts are empowered to grant mandatory injunctions and such other and further equitable relief as they deem appropriate in the enforcement of such final orders of the Commission.

(m) Civil actions for recovery of penalties for knowing violations of rules and cease and desist orders respecting unfair or deceptive acts or practices; jurisdiction; maximum amount of penalties; continuing violations; de novo determinations; compromise or settlement procedure

- (1) (A) The Commission may commence a civil action to recover a civil penalty in a district court of the United States against any person, partnership, or corporation which violates any rule under this subchapter respecting unfair or deceptive acts or practices (other than an interpretive rule or a rule violation of which the Commission has provided is not an unfair or deceptive act or practice in violation of subsection (a)(1) of this section) with actual knowledge or knowledge fairly implied on the basis of objective circumstances that such act is unfair or deceptive and is prohibited by such rule. In such action, such person, partnership, or corporation shall be liable for a civil penalty of not more than \$10,000 for each violation.
- (B) If the Commission determines in a proceeding under subsection (b) of this section that any act or practice is unfair or deceptive, and issues a final cease and desist order, other than a consent order, with respect to such act or practice, then the Commission may commence a civil action to obtain a civil penalty in a district court of the United States against any person, partnership, or corporation which engages in such act or practice—
- (1) after such cease and desist order becomes final (whether or not such person, partnership, or corporation was subject to such cease and desist order), and
- (2) with actual knowledge that such act or practice is unfair or deceptive and is unlawful under subsection (a)(1) of this section.

In such action, such person, partnership, or corporation shall be liable for a civil penalty of not more than \$10,000 for each violation.

- (C) In the case of a violation through continuing failure to comply with a rule or with subsection (a)(1) of this section, each day of continuance of such failure shall be treated as a separate violation, for purposes of subparagraphs (A) and (B). In determining the amount of such a civil penalty, the court shall take into account the degree of culpability, any history of prior such conduct, ability to pay, effect on ability to continue to do business, and such other matters as justice may require.
- (2) If the cease and desist order establishing that the act or practice is unfair or deceptive was not issued against the defendant in a civil penalty action under paragraph (1)(B) the issues of fact in such action against such defendant shall be tried de novo. Upon request of any party to such an action against such defendant, the court shall also review the determination of law made by the Commission in the proceeding under subsection (b) of this section that the act or practice which was the subject of such proceeding constituted an unfair or deceptive act or practice in violation of subsection (a) of this section.
- (3) The Commission may compromise or settle any action for a civil penalty if such compromise or settlement is accompanied by a public statement of its reasons and is approved by the court.

(n) Standard of proof; public policy considerations

The Commission shall have no authority under this section or section 57a of this title to declare unlawful an act or practice on the grounds that such act or practice is unfair unless the act or practice

NB: This unofficial compilation of the U.S. Code is current as of Jan. 4, 2012 (see <http://www.law.cornell.edu/uscode/uscprint.html>).

causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition. In determining whether an act or practice is unfair, the Commission may consider established public policies as evidence to be considered with all other evidence. Such public policy considerations may not serve as a primary basis for such determination.

Footnotes

¹ So in original. Probably should be “clause”.

(Sept. 26, 1914, ch. 311, § 5, 38 Stat. 719; Mar. 21, 1938, ch. 49, § 3, 52 Stat. 111; June 23, 1938, ch. 601, title XI, § 1107(f), 52 Stat. 1028; June 25, 1948, ch. 646, § 32(a), 62 Stat. 991; May 24, 1949, ch. 139, § 127, 63 Stat. 107; Mar. 16, 1950, ch. 61, § 4(c), 64 Stat. 21; July 14, 1952, ch. 745, § 2, 66 Stat. 632; Pub. L. 85–726, title XIV, §§ 1401(b), 1411, Aug. 23, 1958, 72 Stat. 806, 809; Pub. L. 85–791, § 3, Aug. 28, 1958, 72 Stat. 942; Pub. L. 85–909, § 3, Sept. 2, 1958, 72 Stat. 1750; Pub. L. 86–507, § 1(13), June 11, 1960, 74 Stat. 200; Pub. L. 93–153, title IV, § 408(c), (d), Nov. 16, 1973, 87 Stat. 591, 592; Pub. L. 93–637, title II, §§ 201(a), 204 (b), 205 (a), Jan. 4, 1975, 88 Stat. 2193, 2200; Pub. L. 94–145, § 3, Dec. 12, 1975, 89 Stat. 801; Pub. L. 96–37, § 1(a), July 23, 1979, 93 Stat. 95; Pub. L. 96–252, § 2, May 28, 1980, 94 Stat. 374; Pub. L. 97–290, title IV, § 403, Oct. 8, 1982, 96 Stat. 1246; Pub. L. 98–620, title IV, § 402(12), Nov. 8, 1984, 98 Stat. 3358; Pub. L. 100–86, title VII, § 715(a)(1), Aug. 10, 1987, 101 Stat. 655; Pub. L. 103–312, §§ 4, 6, 9, Aug. 26, 1994, 108 Stat. 1691, 1692, 1695; Pub. L. 109–455, § 3, Dec. 22, 2006, 120 Stat. 3372.)

Amendment of Section

For termination of amendment by section 13 of Pub. L. 109–455, see Termination Date of 2006 Amendment note below.

References in Text

The Packers and Stockyards Act, 1921, as amended, referred to in subsec. (a)(2), is act Aug. 15, 1921, ch. 64, 42 Stat. 159, as amended, which is classified to chapter 9 (§ 181 et seq.) of Title 7, Agriculture. For complete classification of this Act to the Code, see section 181 of Title 7 and Tables.

Codification

In subsec. (a)(2), “part A of subtitle VII of title 49” substituted for “the Federal Aviation Act of 1958 [49 App. U.S.C. 1301 et seq.]” on authority of Pub. L. 103–272, § 6(b), July 5, 1994, 108 Stat. 1378, the first section of which enacted subtitles II, III, and V to X of Title 49, Transportation.

In subsec. (c), “section 1254 of title 28” substituted for “section 240 of the Judicial Code [28 U.S.C. 347]” on authority of act June 25, 1948, ch. 646, 62 Stat. 869, the first section of which enacted Title 28, Judiciary and Judicial Procedure.

Amendments

2006—Subsec. (a)(4). Pub. L. 109–455, §§ 3, 13, temporarily added par. (4). See Termination Date of 2006 Amendment note below.

1994—Subsec. (g)(1). Pub. L. 103–312, § 6(d), substituted a period for “; or” at end.

Subsec. (g)(2). Pub. L. 103–312, § 6(a), amended par. (2) generally. Prior to amendment, par. (2) read as follows: “Upon the expiration of the time allowed for filing a petition for certiorari, if the order of the Commission has been affirmed, or the petition for review dismissed by the court of appeals, and no petition for certiorari has been duly filed; or”.

Subsec. (g)(3). Pub. L. 103–312, § 6(b), amended par. (3) generally. Prior to amendment, par. (3) read as follows: “Upon the denial of a petition for certiorari, if the order of the Commission has been affirmed or the petition for review dismissed by the court of appeals; or”.

Subsec. (g)(4). Pub. L. 103–312, § 6(c), amended par. (4) generally. Prior to amendment, par. (4) read as follows: “Upon the expiration of thirty days from the date of issuance of the mandate of the Supreme Court, if such Court directs that the order of the Commission be affirmed or the petition for review dismissed.”

NB: This unofficial compilation of the U.S. Code is current as of Jan. 4, 2012 (see <http://www.law.cornell.edu/uscode/uscpri.html>).

Subsec. (m)(1)(B). Pub. L. 103-312, § 4(a), inserted “, other than a consent order,” after “a final cease and desist order” in introductory provisions.

Subsec. (m)(2). Pub. L. 103-312, § 4(b), inserted at end “Upon request of any party to such an action against such defendant, the court shall also review the determination of law made by the Commission in the proceeding under subsection (b) of this section that the act or practice which was the subject of such proceeding constituted an unfair or deceptive act or practice in violation of subsection (a) of this section.”

Subsec. (n). Pub. L. 103-312, § 9, added subsec. (n).

1987—Subsec. (a)(2). Pub. L. 100-86 inserted “Federal credit unions described in section 57a (f)(4) of this title,” after “section 57a (f)(3) of this title,”.

1984—Subsec. (e). Pub. L. 98-620 struck out provision that such proceedings in the court of appeals had to be given precedence over other cases pending therein, and had to be in every way expedited.

1982—Subsec. (a)(3). Pub. L. 97-290 added par. (3).

1980—Subsec. (b). Pub. L. 96-252 added cl. (2) and provision following cl. (2) requiring that the Commission determine whether to alter, modify, or set aside any order of the Commission in response to a request made by a person, partnership, or corporation under paragraph (2) not later than 120 days after the date of the filing of such request.

1979—Subsec. (a)(2). Pub. L. 96-37 added savings and loan institutions described in section 57a (f)(3) of this title to the enumeration of entities exempted from the Commission’s power to prevent the use of unfair methods of competition and unfair or deceptive acts or practices.

1975—Pub. L. 93-637, § 201(a), substituted “in or affecting commerce” for “in commerce” wherever appearing.

Subsec. (a). Pub. L. 94-145 struck out pars. (2) to (5) which permitted fair trade pricing of articles for retail sale and State enactment of nonsigner provisions, and redesignated par. (6) as (2).

Subsec. (m). Pub. L. 93-637, §§ 204(b), 205 (a), added subsec. (m). Former subsec. (m), relating to the election by the Commission to appear in its own name after notifying and consulting with and giving the Attorney General 10 days to take the action proposed by the Commission, was struck out.

1973—Subsec. (l). Pub. L. 93-153, § 408(c), raised the maximum civil penalty for each violation to \$10,000 and inserted provisions empowering the United States District Courts to grant mandatory injunctions and such other and further equitable relief as they might deem appropriate for the enforcement of final Commission orders.

Subsec. (m). Pub. L. 93-153, § 408(d), added subsec. (m).

1960—Subsec. (f). Pub. L. 86-507 substituted “mailing a copy thereof by registered mail or by certified mail” for “registering and mailing a copy thereof”, and “mailed by registered mail or by certified mail” for “registered and mailed”.

1958—Subsec. (a)(6). Pub. L. 85-909 substituted “persons, partnerships, or corporations insofar as they are subject to the Packers and Stockyards Act, 1921, as amended,” for “persons, partnerships or corporations subject to the Packers and Stockyards Act, 1921,”.

Pub. L. 85-726, § 1411, substituted “Federal Aviation Act of 1958” for “Civil Aeronautics Act of 1938”.

Subsec. (b). Pub. L. 85-791, § 3(a), struck out “the transcript of” before “the record in the proceeding” in sixth sentence.

Subsec. (c). Pub. L. 85-791, § 3(b), in second sentence, substituted “transmitted by the clerk of the court to” for “served upon”, and “Commission shall file in the court the record in the proceeding, as provided in section 2112 of title 28” for “Commission forthwith shall certify and file in the court a transcript of the entire record in the proceeding, including all the evidence taken and the report and order of the Commission”, and which, in third sentence struck out “and transcript” after “petition”, inserted “concurrently with the Commission until the filing of the record” and struck out “upon the pleadings, evidence, and proceedings set forth in such transcript” before “a decree affirming”.

Subsec. (d). Pub. L. 85-791, § 3(c), substituted “Upon the filing of the record with it the” for “The”.

1952—Subsec. (a). Act July 14, 1952, amended subsec. (a) generally to permit fair trade pricing of articles for retail sale.

1950—Subsec. (l). Act Mar. 16, 1950, inserted last sentence to make each separate violation of a cease and desist order as a separate offense, except that each day of a continuing failure to obey a final order shall be a separate offense.

1938—Subsec. (a). Act June 23, 1938, inserted “air carriers and foreign air carriers subject to chapter 9 of title 49” in second par.

Act Mar. 21, 1938, amended section generally.

Change of Name

Act June 25, 1948, eff. Sept. 1, 1948, as amended by act May 24, 1949, substituted “court of appeals” for “circuit court of appeals”.

Termination Date of 2006 Amendment

Amendment by Pub. L. 109–455 to cease to have effect 7 years after Dec. 22, 2006, see section 13 of Pub. L. 109–455, set out as a note under section 44 of this title.

Effective Date of 1994 Amendment

Pub. L. 103–312, § 15, Aug. 26, 1994, 108 Stat. 1697, provided that:

“(a) In General.—Except as provided in subsections (b), (c), (d), and (e), the provisions of this Act [enacting section 57b–5 of this title, amending this section and sections 53, 57a, 57b–1, 57b–2, 57c, and 58 of this title, and enacting provisions set out as notes under sections 57c and 58 of this title] shall take effect on the date of enactment of this Act [Aug. 26, 1994].

“(b) Applicability of Section 5.—The amendment made by section 5 of this Act [amending section 57a of this title] shall apply only to rulemaking proceedings initiated after the date of enactment of this Act. Such amendment shall not be construed to affect in any manner a rulemaking proceeding which was initiated before the date of enactment of this Act [Aug. 26, 1994].

“(c) Applicability of Section 6.—The amendments made by section 6 of this Act [amending this section] shall apply only with respect to cease and desist orders issued under section 5 of the Federal Trade Commission Act (15 U.S.C. 45) after the date of enactment of this Act [Aug. 26, 1994]. These amendments shall not be construed to affect in any manner a cease and desist order which was issued before the date of enactment of this Act.

“(d) Applicability of Sections 7 and 8.—The amendments made by sections 7 and 8 of this Act [amending sections 57b–1 and 57b–2 of this title] shall apply only with respect to compulsory process issued after the date of enactment of this Act [Aug. 26, 1994].

“(e) Applicability of Section 9.—The amendments made by section 9 of this Act [amending this section] shall apply only with respect to cease and desist orders issued under section 5 of the Federal Trade Commission Act (15 U.S.C. 45), or to rules promulgated under section 18 of the Federal Trade Commission Act (15 U.S.C. 57a) after the date of enactment of this Act [Aug. 26, 1994]. These amendments shall not be construed to affect in any manner a cease and desist order which was issued, or a rule which was promulgated, before the date of enactment of this Act. These amendments shall not be construed to affect in any manner a cease and desist order issued after the date of enactment of this Act, if such order was issued pursuant to remand from a court of appeals or the Supreme Court of an order issued by the Federal Trade Commission before the date of enactment of this Act.”

Effective Date of 1984 Amendment

Amendment by Pub. L. 98–620 not applicable to cases pending on Nov. 8, 1984, see section 403 of Pub. L. 98–620, set out as an Effective Date note under section 1657 of Title 28, Judiciary and Judicial Procedure.

Effective Date of 1980 Amendment

Pub. L. 96–252, § 23, May 28, 1980, 94 Stat. 397, provided that: “The provisions of this Act [enacting sections 57a–1 and 57b–1 to 57b–4 of this title, amending this section and sections 46, 50, 57a, 57c, and 58 of this title, and enacting provisions set out as notes under sections 46, 57a, 57a–1, 57c, and 58 of this title], and the amendments made by this Act, shall take effect on the date of the enactment of this Act [May 28, 1980].”

Effective Date of 1975 Amendments

Amendment by Pub. L. 94–145 effective upon expiration of ninety-day period beginning on Dec. 12, 1975, see section 4 of Pub. L. 94–145, set out as a note under section 1 of this title.

Amendment by section 204(b) of Pub. L. 93–637 not applicable to any civil action commenced before Jan. 4, 1975, see section 204(c) of Pub. L. 93–637, set out as a note under section 56 of this title.

Pub. L. 93–637, § 205(b), Jan. 4, 1975, 88 Stat. 2201, provided that: “The amendment made by subsection (a) of this section [amending this section] shall not apply to any violation, act, or practice to the extent that such violation, act, or practice occurred before the date of enactment of this Act [Jan. 4, 1975].”

NB: This unofficial compilation of the U.S. Code is current as of Jan. 4, 2012 (see <http://www.law.cornell.edu/uscode/uscpint.html>).

Effective Date of 1958 Amendment

Amendment by Pub. L. 85-726 effective on 60th day following the date on which the Administrator of the Federal Aviation Agency first appointed under Pub. L. 85-726 qualifies and takes office, see section 1505(2) of Pub. L. 85-726. The Administrator was appointed, qualified, and took office on Oct. 31, 1958.

Effective Date of 1950 Amendment

Amendment by act Mar. 16, 1950, effective July 1, 1950, see note set out under section 347 of Title 21, Food and Drugs.

Transfer of Functions

For transfer of functions of Federal Trade Commission, with certain exceptions, to Chairman of such Commission, see Reorg. Plan No. 8 of 1950, § 1, eff. May 24, 1950, 15 F.R. 3175, 64 Stat. 1264, set out under section 41 of this title.

Congressional Findings and Declaration of Purpose Covering Grant of District Subpena Enforcement Authority and Authority To Grant Preliminary Injunctive Relief

Pub. L. 93-153, § 408(a), (b), Nov. 16, 1973, 87 Stat. 591, provided that:

“(a)(1) The Congress hereby finds that the investigative and law enforcement responsibilities of the Federal Trade Commission have been restricted and hampered because of inadequate legal authority to enforce subpoenas and to seek preliminary injunctive relief to avoid unfair competitive practices.

“(2) The Congress further finds that as a direct result of this inadequate legal authority significant delays have occurred in a major investigation into the legality of the structure, conduct, and activities of the petroleum industry, as well as in other major investigations designed to protect the public interest.

“(b) It is the purpose of this Act [amending this section and sections 46, 53, and 56 of this title] to grant the Federal Trade Commission the requisite authority to insure prompt enforcement of the laws the Commission administers by granting statutory authority to directly enforce subpoenas issued by the Commission and to seek preliminary injunctive relief to avoid unfair competitive practices.”

Purpose of Act July 14, 1952

Act July 14, 1952, ch. 745, § 1, 66 Stat. 631, provided: “That it is the purpose of this Act [amending this section] to protect the rights of States under the United States Constitution to regulate their internal affairs and more particularly to enact statutes and laws, and to adopt policies, which authorize contracts and agreements prescribing minimum or stipulated prices for the resale of commodities and to extend the minimum or stipulated prices prescribed by such contracts and agreements to persons who are not parties thereto. It is the further purpose of this Act to permit such statutes, laws, and public policies to apply to commodities, contracts, agreements, and activities in or affecting interstate or foreign commerce.”

Read 11/3

0823099

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION

COMMISSIONERS: Jon Leibowitz, Chairman
Pamela Jones Harbour
William E. Kovacic
J. Thomas Rosch

In the Matter of

SEARS HOLDINGS MANAGEMENT
CORPORATION,
a corporation.

DOCKET NO. C-4264

COMPLAINT

The Federal Trade Commission, having reason to believe that Sears Holdings Management Corporation, a corporation, has violated the provisions of the Federal Trade Commission Act, and it appearing to the Commission that this proceeding is in the public interest, alleges:

1. Respondent Sears Holdings Management Corporation ("respondent" or "SHMC") is a Delaware corporation with its principal office or place of business at 3333 Beverly Road, Hoffman Estates, Illinois 60179. SHMC, a subsidiary of Sears Holdings Corporation ("SHC") with shares owned by Sears, Roebuck and Co. and Kmart Management Corporation, handles marketing operations for the Sears Roebuck and Kmart retail stores, and operates the sears.com and kmart.com retail Internet websites.
2. The acts and practices of respondent, as alleged herein, have been in or affecting commerce, as "commerce" is defined in Section 4 of the Federal Trade Commission Act.
3. From on or about April 2007 through on or about January 2008, SHMC disseminated or caused to be disseminated via the Internet a software application for consumers to download and install onto their computers (the "Application"). The Application was created, developed, and managed for respondent by a third party in connection with SHMC's "My SHC Community" market research program.
4. The Application, when installed, runs in the background at all times on consumers' computers and transmits tracked information, including nearly all of the Internet behavior that occurs on those computers, to servers maintained on behalf of respondent. Information collected and transmitted includes: web browsing, filling shopping baskets, transacting business during

secure sessions, completing online application forms, checking online accounts, and, through select header information, use of web-based email and instant messaging services.

5. SHMC, during the relevant time period, presented fifteen out of every hundred visitors to the sears.com and kmart.com websites with a "My SHC Community" pop-up box (Exhibit A) that said:

Ever wish you could talk directly to a retailer? Tell them about the products, services and offers that would really be right for you?

If you're interested in becoming part of something new, something different, we'd like to invite you to become a member of My SHC Community. My SHC Community, sponsored by Sears Holdings Corporation, is a dynamic and highly interactive on-line community. It's a place where your voice is heard and your opinion matters, and what you want and need counts!

The pop-up box made no mention of the Application. Likewise, the general "Privacy Policy" statement accessed via the hyperlink in the pop-up box did not mention the Application.

6. The pop-up box message further invited consumers to enter their email address to receive a follow-up email from SHMC with more information. Subsequently, invitation messages (Exhibit B) were emailed to those consumers who supplied their email address. These emails stated, in pertinent part:

From shopping, current events, social networking, to entertainment and email, it seems that the Internet is playing a bigger and bigger role in our daily lives these days.

If you're interested in becoming part of something new, something different, we'd like to invite you to join a new and exciting online community; My SHC Community, sponsored by Sears Holdings Corporation. *Membership is absolutely free!*

My SHC Community is a dynamic and highly interactive online community. It's a place where your voice is heard and your opinion matters, and what you want and need counts! As a member of My SHC Community, you'll partner directly with the retail industry. You'll participate in exciting, engaging and on-going interactions – always on your terms and always by your choice. My SHC Community gives you the chance to help shape the future by sharing and receiving information about the products, services and offers that would really be right for you.

→ To become a member of My SHC Community, we simply ask you to complete the registration process which includes providing us with your contact information as well as answering a series of profile questions that will help us get to know you better. You'll also be asked to take a few minutes to download software that is powered by (VoiceFive). This research software will confidentially track your online browsing. This will help us better understand you and your needs, enabling us to create more relevant future offerings for you, other community members, and eventually all shoppers. You can uninstall the software at any time through the Add/Remove program utility on your computer. During the registration process, you'll learn more about this application software and you'll always have the opportunity to ask any and every question you may have.

Once you're a member of My SHC Community, you'll regularly interact with My SHC Community members as well as employees of Sears Holdings Corporation through special online engagements, surveys, chats and other fun and informative online techniques. We'll ask you to journal your shopping and purchasing behavior. Again, this will be when you want and how you want to record it – always on your terms and always by your choice. We'll also collect information on your internet usage. Community engagements are always fun and always voluntary!

The email invitation message then described what consumers would receive in exchange for becoming a member of the My SHC Community, including a \$10 payment for joining the "online community," contingent upon the consumer retaining the Application on his or her computer for at least one month. Consumers who wished to proceed further would need to click a button, at the bottom, center portion of the invitation email, that said "Join Today!"

7. Consumers who clicked on the "Join Today!" button in the email invitation were directed to a landing page (Exhibit C) that restated many of the aforementioned representations about the potential interactions between members and the "community" and about the putative benefits of membership. The landing page did not mention the Application.

8. Consumers who clicked on the "Join Today" button in the landing page were directed to a registration page (Exhibit D). To complete registration, consumers needed to enter information, including their name, address, age, and email address. Below the fields for entering information, the registration page presented a "Privacy Statement and User License Agreement" ("PSULA") in a "scroll box" that displayed ten lines of the multi-page document at a time ("Printable version" attached as Exhibit E). A description of the Application's specific functions begins on approximately the 75th line down in the scroll box:

Computer hardware, software, and other configuration information: Our application may collect certain basic hardware, software, computer configuration and application usage information about the computer on which you install our application, including such data as the speed of the computer processor, its memory capacities and Internet connection speed. In addition, our application may report on devices connected to your computer, such as the type of printer or router you may be using.

Internet usage information: Once you install our application, it monitors all of the Internet behavior that occurs on the computer on which you install the application, including both your normal web browsing and the activity that you undertake during secure sessions, such as filling a shopping basket, completing an application form or checking your online accounts, which may include personal financial or health information. We may use the information that we monitor, such as name and address, for the purpose of better understanding your household demographics; however we make commercially viable efforts to automatically filter confidential personally identifiable information such as UserID, password, credit card numbers, and account numbers. Inadvertently, we may collect such information about our panelists; and when this happens, we make commercially viable efforts to purge our database of such information.

It was disclosed

The software application also tracks the pace and style with which you enter information online (for example, whether you click on links, type in webpage names, or use shortcut keys), the usage of cookies, and statistics about your use of online applications (for example, it may observe that during a given period of use of a computer, the computer downloaded X number of bytes of data using a particular Internet enabled gaming application).

Please note: Our application does not examine the text of your instant messages or e-mail messages. We may, however, review select e-mail header information from web-based e-mails as a way to verify your contact information and online usage information.

What?

The PSULA went on to describe how the information the Application would collect was transmitted to respondent's servers, how it might be used, and how it was maintained. It also described how consumers could stop participating in the online community and remove the Application from their computers. Respondent stated in the PSULA that it reserved the right to continue to use information collected prior to a consumer's "resignation."

9. Below the scroll box on the registration page was a link that consumers could click to access a printable version of the PSULA, and a blank checkbox next to the statement: "I am the authorized user of this computer and I have read, agree to, and have obtained the agreement of

all computer users to the terms and conditions of the Privacy Statement and User License Agreement.” To continue with the registration process, consumers needed to check the box and click the “Next” button at the bottom of the registration page.

10. Consumers who completed the required information, checked the box, and clicked the “Next” button on the registration page, were directed to an installation page (Exhibit F) that explained the Application download and installation process. Consumers were required to click a “Next” button to begin the download, and then click an “Install” or “Yes” button in a “security warning” dialog box to install the Application. Nothing on the installation page provided information on the Application.

11. When installed, the Application functioned and transmitted information substantially as described in the PSULA. The Application, when installed, would run in the background at all times on consumers’ computers. Although the Application would be listed (as “mySHC Community”) in the “All Programs” menu and “Add/Remove” utilities of those computers, and the Application’s executable file name (“srhc.exe”) would be listed as a running process in Windows Task Manager, the Application would display to users of those computers no visible indication, such as a desktop or system tray icon, that it was running.

12. The Application transmitted, in real time, tracked information to servers maintained on behalf of respondent. The tracked information included not only information about websites consumers visited and links that they clicked, but also the text of secure pages, such as online banking statements, video rental transactions, library borrowing histories, online drug prescription records, and select header fields that could show the sender, recipient, subject, and size of web-based email messages.

13. Through the means described in paragraphs 3-12, respondent has represented, expressly or by implication, that the Application would track consumers’ “online browsing.” Respondent failed to disclose adequately that the software application, when installed, would: monitor nearly all of the Internet behavior that occurs on consumers’ computers, including information exchanged between consumers and websites other than those owned, operated, or affiliated with respondent, information provided in secure sessions when interacting with third-party websites, shopping carts, and online accounts, and headers of web-based email; track certain non-Internet-related activities taking place on those computers; and transmit nearly all of the monitored information (excluding selected categories of filtered information) to respondent’s remote computer servers. These facts would be material to consumers in deciding to install the software. Respondent’s failure to disclose these facts, in light of the representations made, was, and is, a deceptive practice.

14. The acts and practices of respondent as alleged in this complaint constitute unfair or deceptive acts or practices in or affecting commerce in violation of Section 5(a) of the Federal Trade Commission Act.

THEREFORE, the Federal Trade Commission this thirty-first day of August, 2009, has issued this complaint against respondent.

By the Commission.

Donald S. Clark
Secretary

Read 11/3

0823099

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION

COMMISSIONERS: Jon Leibowitz, Chairman
Pamela Jones Harbour
William E. Kovacic
J. Thomas Rosch

In the Matter of)
)
)

SEARS HOLDINGS MANAGEMENT)
CORPORATION,)
a corporation.)

DOCKET NO. C-4264

DECISION AND ORDER

The Federal Trade Commission ("Commission") having initiated an investigation of certain acts and practices of the Respondent named in the caption hereof, and the Respondent having been furnished thereafter with a copy of a draft complaint that the Bureau of Consumer Protection proposed to present to the Commission for its consideration and which, if issued by the Commission, would charge the Respondent with violation of the Federal Trade Commission Act, 15 U.S.C § 45 et seq.; and

The Respondent, its attorney, and counsel for the Commission having thereafter executed an agreement containing a consent order ("consent agreement"), an admission by the Respondent of all the jurisdictional facts set forth in the aforesaid draft complaint, a statement that the signing of said consent agreement is for settlement purposes only and does not constitute an admission by the Respondent that the law has been violated as alleged in the complaint, or that the facts as alleged in such complaint, other than jurisdictional facts, are true, and waivers and other provisions as required by the Commission's Rules; and

The Commission having thereafter considered the matter and having determined that it has reason to believe that the Respondent has violated the said Act, and that a complaint should issue stating its charges in that respect, and having thereupon accepted the executed consent agreement and placed such consent agreement on the public record for a period of thirty (30) days, and having duly considered the comments filed thereafter by interested persons pursuant to

Section 2.34 of its Rules, now in further conformity with the procedure prescribed in Section 2.34 of its Rules, the Commission hereby issues its complaint, makes the following jurisdictional findings and enters the following order:

1. Respondent Sears Holdings Management Corporation is a Delaware corporation with its principal office or place of business at 3333 Beverly Road, Hoffman Estates, Illinois 60179.
2. The Federal Trade Commission has jurisdiction of the subject matter of this proceeding and of the Respondent, and the proceeding is in the public interest.

ORDER

DEFINITIONS

For purposes of this Order, the following definitions shall apply:

1. Unless otherwise specified, “respondent” shall mean Sears Holdings Management Corporation, its successors and assigns, and its officers, agents, representatives, and employees.
2. “Commerce” shall mean as defined in Section 4 of the Federal Trade Commission Act, 15 U.S.C. § 44.
3. “Computer” shall mean any desktop or laptop computer, handheld device, telephone, or other electronic product or device that has a platform on which to download, install, or run any software program, code, script, or other content and to play any digital audio, visual, or audiovisual content.
4. “Tracking Application” shall mean any software program or application disseminated by or on behalf of respondent, its subsidiaries or affiliated companies, that is capable of being installed on consumers’ computers and used by or on behalf of respondent to monitor, record, or transmit information about activities occurring on computers on which it is installed, or about data that is stored on, created on, transmitted from, or transmitted to the computers on which it is installed.
5. “Affected Consumers” shall mean persons who, prior to the date of issuance of this order, downloaded and installed a Tracking Application on a computer in connection with the My SHC Community program or “on-line community.”

6. "Collected Information" shall mean any information or data transmitted from a computer by a Tracking Application, installed prior to the date of issuance of this order, to any computer server owned by, operated by, or operated for the benefit of, Sears Holdings Management Corporation, its subsidiaries, or affiliated companies.

7. "Clearly and prominently" shall mean:

- A. In textual communications (*e.g.*, printed publications or words displayed on the screen of a computer), the required disclosures are of a type, size, and location sufficiently noticeable for an ordinary consumer to read and comprehend them, in print that contrasts with the background on which they appear;
- B. In communications disseminated orally or through audible means (*e.g.*, radio or streaming audio), the required disclosures are delivered in a volume and cadence sufficient for an ordinary consumer to hear and comprehend them;
- C. In communications disseminated through video means (*e.g.*, television or streaming video), the required disclosures are in writing in a form consistent with subparagraph (A) of this definition and shall appear on the screen for a duration sufficient for an ordinary consumer to read and comprehend them, and in the same language as the predominant language that is used in the communication;
- D. In communications made through interactive media, such as the Internet, online services, and software, the required disclosures are unavoidable and presented in a form consistent with subparagraph (A) of this definition, in addition to any audio or video presentation of them; and
- E. In all instances, the required disclosures are presented in an understandable language and syntax, and with nothing contrary to, inconsistent with, or in mitigation of the disclosures used in any communication of them.

I.

IT IS ORDERED that respondent, directly or through any corporation, subsidiary, division, or other device, in connection with the advertising, promotion, offering for sale, sale, or dissemination of any Tracking Application, in or affecting commerce, shall, prior to the consumer downloading or installing it:

- A. Clearly and prominently, and prior to the display of, and on a separate screen from, any final "end user license agreement," "privacy policy," "terms of use" page, or similar document, disclose: (1) all the types of data that the Tracking Application will monitor, record, or transmit, including but not limited to whether

the data may include information from the consumer's interactions with a specific set of websites or from a broader range of Internet interaction, whether the data may include transactions or information exchanged between the consumer and third parties in secure sessions, interactions with shopping baskets, application forms, or online accounts, and whether the information may include personal financial or health information; (2) how the data may be used; and (3) whether the data may be used by a third party; and

- B. Obtain express consent from the consumer to the download or installation of the Tracking Application and the collection of data by having the consumer indicate assent to those processes by clicking on a button or link that is not pre-selected as the default option and that is clearly labeled or otherwise clearly represented to convey that it will initiate those processes, or by taking a substantially similar action.

II.

IT IS FURTHER ORDERED that respondent, directly or through any corporation, subsidiary, division, or other device, shall:

- A. Within thirty (30) days after the date of service of this order, notify Affected Consumers that they have installed respondent's Tracking Application on their computers, that the Tracking Application collects and transmits to respondent and others the data described in the My SHC Community "Privacy Statement & User License Agreement," and notify them how to uninstall the Tracking Application. Notification shall be by the following means:
1. For two (2) years after the date of service of this order, posting of a clear and prominent notice on the www.myshccommunity.com website; and
 2. For three (3) years after the date of service of this order, informing Affected Consumers who complain or inquire about any Tracking Application; and
- B. Provide prompt, toll-free, telephonic and electronic mail support to help Affected Consumers uninstall any Tracking Application.

III.

IT IS FURTHER ORDERED that respondent, directly or through any corporation, subsidiary, division, or other device, shall:

- A. Within three (3) days after the date of service of this order, cease collecting any data transmitted by any Tracking Application installed before the date of service of this Order; and
- B. Within five (5) days after the date of service of this order, destroy any Collected Information.

IV.

IT IS FURTHER ORDERED that respondent, Sears Holdings Management Corporation, and its successors and assigns, shall maintain, and upon request make available to the Federal Trade Commission for inspection and copying, a print or electronic copy of each document relating to compliance with the terms and provisions of this order, including but not limited to:

- A. For a period of four (4) years, any documents, whether prepared by or on behalf of respondent, that:
 - 1. Comprise or relate to complaints or inquiries, whether received directly, indirectly, or through any third party, concerning a Tracking Application, and any responses to those complaints or inquiries;
 - 2. Are reasonably necessary to demonstrate full compliance with each provision of this order, including but not limited to, all documents obtained, created, generated, or which in any way relate to the requirements, provisions, terms of this order, and all reports submitted to the Commission pursuant to this order; and
 - 3. Contradict, qualify, or call into question respondent's compliance with this order; and
- B. For a period of four (4) years after the last public dissemination thereof, all advertisements, terms of use, end-user license agreements, frequently asked questions, privacy policies, and similar documents relating to respondent's dissemination of any Tracking Application.

V.

IT IS FURTHER ORDERED that respondent, Sears Holdings Management Corporation, and its successors and assigns, shall deliver a copy of this order to all current and future principals, officers, directors, managers, employees, agents, and representatives having responsibilities with respect to the subject matter of this order. Respondent, Sears Holdings Management Corporation, and its successors and assigns, shall deliver this order to current

personnel within thirty (30) days after the date of service of the order, and to future personnel within thirty (30) days after the person assumes such position or responsibilities.

VI.

IT IS FURTHER ORDERED that respondent, Sears Holdings Management Corporation, and its successors and assigns, shall notify the Commission at least thirty (30) days prior to any change in the entity that may affect compliance obligations arising under this order, including but not limited to, a dissolution, assignment, sale, merger, or other action that would result in the emergence of a successor entity; the creation or dissolution of a subsidiary, parent, or affiliate that engages in any acts or practices subject to this order; the proposed filing of a bankruptcy petition; or a change in the entity name or address. *Provided, however*, that with respect to any proposed change in the entity about which respondent, Sears Holdings Management Corporation, and its successors and assigns, learns less than thirty (30) days prior to the date such action is to take place, respondent, Sears Holdings Management Corporation, and its successors and assigns, shall notify the Commission as soon as is practicable after obtaining such knowledge. All notices required by this Part shall be sent by certified mail to the Associate Director, Division of Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Ave., N.W., Washington, D.C. 20580.

VII.

IT IS FURTHER ORDERED that respondent, Sears Holdings Management Corporation, and its successors and assigns, shall, within sixty (60) days after service of this order, and at such other times as the Federal Trade Commission may require, file with the Commission a report, in writing, setting forth the manner and form in which respondent has complied with this order.

VIII.

This order will terminate on August 31, 2029, or twenty (20) years from the most recent date that the United States or the Federal Trade Commission files a complaint (with or without an accompanying consent decree) in federal court alleging any violation of the order, whichever comes later; *provided, however*, that the filing of such a complaint will not affect the duration of:

- A. Any Part of this order that terminates in less than twenty (20) years;
- B. This order's application to any respondent that is not named as a defendant in such a complaint; and
- C. This order if such complaint is filed after the order has terminated pursuant to this Part.

Provided, further, that if such complaint is dismissed or a federal court rules that the respondent

did not violate any provision of the order, and the dismissal or ruling is either not appealed or upheld *on* appeal, then the order will terminate according to this Part as though the complaint had never been filed, except that this order will not terminate between the date such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

By the Commission.

Donald S. Clark
Secretary

SEAL:
ISSUED: August 31, 2009

Read 11/3

Before the
Federal Trade Commission
Washington, DC

In the Matter of)

Google, Inc.)
)
)
)
_____)

Complaint, Request for Investigation, Injunction, and Other Relief

I. Introduction

1. This complaint concerns an attempt by Google, Inc., the provider of a widely used email service to convert the private, personal information of Gmail subscribers into public information for the company's social network service (Google Buzz). This change in business practices and service terms violated user privacy expectations, diminished user privacy, contradicted Google's own privacy policy, and may have also violated federal wiretap laws. In some instances, there were clear harms to service subscribers. These business practices are Unfair and Deceptive Trade Practices, subject to review by the Federal Trade Commission (the "Commission") under section 5 of the Federal Trade Commission Act.
2. These business practices impact more than 37 million users of Gmail who fall within the jurisdiction of the United States Federal Trade Commission.¹
3. EPIC urges the Commission to investigate Google, determine the extent of the harm to consumer privacy and safety, require Google to provide Gmail users with opt-in consent to the Google Buzz service, require Google to give Gmail users meaningful control over personal information, require Google to provide notice to and request consent from Gmail users before making material changes to their privacy policy in the future, and seek appropriate injunctive and compensatory relief.

How
request
consent?

¹ Erick Schonfeld, *Gmail Nudges Past AOL Email in the U.S. to Take No. 3 Spot*, TechCrunch (Aug. 14, 2009), <http://techcrunch.com/2009/08/14/gmail-nudges-past-aol-email-in-the-us-to-take-no-3-spot/>.

II. Parties

4. The Electronic Privacy Information Center (“EPIC”) is a not-for-profit research center based in Washington, D.C. EPIC focuses on emerging privacy and civil liberties issues and is a leading consumer advocate before the Federal Trade Commission. Among its other activities, EPIC first brought the Commission’s attention to the privacy risks of online advertising.² In 2004, EPIC filed a complaint with the FTC regarding the deceptive practices of data broker firm Choicepoint, calling the Commission’s attention to “data products circumvent[ing] the FCRA, giving businesses, private investigators, and law enforcement access to data that previously had been subjected to Fair Information Practices.”³ As a result of the EPIC complaint, the FTC fined Choicepoint \$15 million.⁴ EPIC initiated the complaint to the FTC regarding Microsoft Passport.⁵ The Commission subsequently required Microsoft to implement a comprehensive information security program for Passport and similar services.⁶ EPIC also filed a complaint with the FTC regarding the marketing of amateur spyware,⁷ which resulted in the issuance of a permanent injunction barring sales of CyberSpy’s “stalker spyware,” over-the-counter surveillance technology sold for individuals to spy on other individuals.⁸

² *In the Matter of DoubleClick*, Complaint and Request for Injunction, Request for Investigation and for Other Relief, before the Federal Trade Commission (Feb. 10, 2000), available at http://epic.org/privacy/internet/ftc/DCLK_complaint.pdf.

³ *In the Matter of Choicepoint*, Request for Investigation and for Other Relief, before the Federal Trade Commission (Dec. 16, 2004), available at <http://epic.org/privacy/choicepoint/fcraltr12.16.04.html>.

⁴ Federal Trade Commission, *ChoicePoint Settles Data Security Breach Charges; to Pay \$10 Million in Civil Penalties*, \$5 Million for Consumer Redress, <http://www.ftc.gov/opa/2006/01/choicepoint.shtm> (last visited Dec. 13, 2009).

⁵ *In the Matter of Microsoft Corporation*, Complaint and Request for Injunction, Request for Investigation and for Other Relief, before the Federal Trade Commission (July 26, 2001), available at http://epic.org/privacy/consumer/MS_complaint.pdf.

⁶ *In the Matter of Microsoft Corporation*, File No. 012 3240, Docket No. C-4069 (Aug. 2002), available at <http://www.ftc.gov/os/caselist/0123240/0123240.shtm>. See also Fed. Trade Comm’n, “Microsoft Settles FTC Charges Alleging False Security and Privacy Promises” (Aug. 2002) (“The proposed consent order prohibits any misrepresentation of information practices in connection with Passport and other similar services. It also requires Microsoft to implement and maintain a comprehensive information security program. In addition, Microsoft must have its security program certified as meeting or exceeding the standards in the consent order by an independent professional every two years.”), available at <http://www.ftc.gov/opa/2002/08/microst.shtm>.

⁷ *In the Matter of Awarenessstech.com, et al.*, Complaint and Request for Injunction, Request for Investigation and for Other relief, before the Federal Trade Commission, available at http://epic.org/privacy/dv/spy_software.pdf.

⁸ *FTC v. Cyberspy Software*, No. 6:08-cv-1872 (D. Fla. Nov. 6, 2008) (unpublished order), available at <http://ftc.gov/os/caselist/0823160/081106cyberspytro.pdf>.

5. In March 2009, EPIC urged the FTC to undertake an investigation of Google and cloud computing.⁹ In that complaint, EPIC specifically warned the FTC that Google had failed to take appropriate steps to safeguard the privacy and security of users. The FTC agreed to review the complaint, stating that it “raises a number of concerns about the privacy and security of information collected from consumers online.”¹⁰ However, to date, the FTC has announced no formal action in the Google cloud computing matter.
6. Google, Inc. was founded in 1998 and is based in Mountain View, California. Google’s headquarters are located at 1600 Amphitheatre Parkway, Mountain View, CA 94043. At all times material to this complaint, Google’s course of business, including the acts and practices alleged herein, has been and is in or affecting commerce, as “commerce” is defined in Section 4 of the Federal Trade Commission Act, 15 U.S.C. § 45.

The Importance of Email Privacy

7. Law, technology, business practice, and custom treat emails and associated information as fundamentally private.
8. While email senders and recipients always have an opportunity to disclose email-related information to third parties, email service providers have a particular responsibility to safeguard the personal information that subscribers provide.
9. Improper disclosure of even a limited amount of subscriber information by an email service provider can be a violation of both state and federal law.
10. An attempt by an email service provider to attempt to convert the personal information of all of its customers into a separate service raises far-reaching concerns for subscribers and implicates both consumer and personal privacy interests.

The Release of Google Buzz

11. Google launched Google Buzz on Tuesday, February 9, 2010. Google Buzz is a social networking tool linked to a user’s Gmail email account, where users “start conversations about the things you find interesting.”¹¹

⁹ *In the Matter of Google, Inc., and Cloud Computing Services*, Request for Investigation and for Other Relief, before the Federal Trade Commission (Mar. 17, 2009), available at <http://epic.org/privacy/cloudcomputing/google/ftc031709.pdf>.

¹⁰ Letter from Eileen Harrington, Acting Director of the FTC Bureau of Consumer Protection, to EPIC (Mar. 18, 2009), available at http://epic.org/privacy/cloudcomputing/google/031809_ftc_ltr.pdf.

¹¹ Todd Jackson, Google Blog post: *Introducing Google Buzz* (Feb. 9, 2010), <http://googleblog.blogspot.com/2010/02/introducing-google-buzz.html>.

12. When Google Buzz was introduced, users could not choose whether to sign up for the tool. According to Google, “No setup needed. Automatically follow the people you email and chat with most in Gmail.”¹²
13. After the launch of Google Buzz, Gmail users who signed into Gmail were confronted with the following screen:

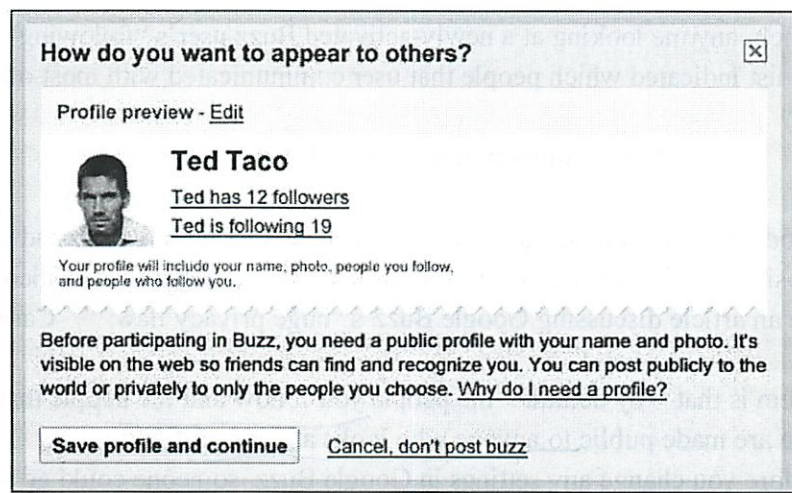


©2010 Google - [Terms of service](#) - [Privacy policy](#)

14. Regardless of whether a user clicked the button labeled “Sweet! Check out Buzz” or “Nah, go to my inbox,” Google Buzz was activated. *lol*
15. Once Google Buzz was activated, the tool automatically populated a user’s “following” lists using that user’s most frequent email contacts.
16. Google Buzz did not warn users that their email contacts would be used to populate their “following” lists.
17. Once users clicked on the “Buzz” tab in Gmail, and then on the text box to share a new post, users were met with the following screen:

When was it actually activated?

¹² Google Buzz Page, <http://www.google.com/buzz> (last visited Feb. 12, 2010).



So only
once click
Buzz tab

18. Once users created public profiles, their "following" and "followed by" lists were also automatically visible to the public.
19. Users were not explicitly warned that their lists would be automatically visible to the public. Instead, each user was told only that "Your profile will include your name, photo, people you follow, and people who follow you." A separate section of the notice stated that the profile was "visible on the web so friends can find and recognize you."
20. Users could hide their "following" and "followed by" lists only by clicking through several links to edit their public profile and then unchecking the box labeled "Display the list of people I'm following and people following me."

photo?

Google's Disclosure of Users' Email Contacts

21. Gmail contact lists routinely include deeply personal information, including the names and email addresses of estranged spouses, current lovers, attorneys and doctors.
22. The frequency with which a user communicates with a given contact is also deeply personal and demonstrates the closeness of the user's relationship with that contact.
23. The activation of Buzz disclosed not only portions of users' contact lists, but more specifically disclosed the contacts with whom users communicate most often.
24. The fact that the auto-following lists were composed of users' most common Gmail contacts was widely known and publicized, as well as easily deduced by individual

did it include "suggested contacts"?

users.¹³ As such, anyone looking at a newly-activated Buzz user's "following" list would know that the list indicated which people that user communicated with most often.

User Opposition to Google Buzz

25. Since the introduction of Google Buzz, Google has been met with widespread criticism and user opposition to the service. Nicholas Carlson, senior editor of the Silicon Alley Insider, wrote an article discussing Google Buzz's "huge privacy flaw."¹⁴ Carlson wrote,

The problem is that—by default—the people you follow and the people that follow you are made public to anyone who looks at your profile. In other words, before you change any settings in Google Buzz, someone could go into your profile and see the people you email and chat with the most.¹⁵

Carlson's article was viewed over 400,000 times, drew in over 250 comments from readers, and was tweeted nearly 6,000 times.

26. CNET writer Molly Wood also wrote against Google Buzz's default settings:

First, you automatically follow everyone in your Gmail contact list, and that information is publicly available in your profile, by default, to everyone who visits your profile. It's available with helpful "follow" links too—wow, you can expand your Buzz network *so fast* by harvesting the personal contact lists of other people!

to explain

Wood continued, speaking of the privacy invasion associated with Google Buzz's attempt to publicize private information in which users have an expectation of privacy:

But I *do* have an expectation of privacy when it comes to my e-mail, and I think that even in this age of social-networking TMI, most people still think of e-mail as a safe place for speaking privately with friends and family. And for Google to come along and broadcast that network to the world without asking first—and force you to turn it off after the fact—is, I think, both shocking and unacceptable.

¹³ See User Opposition to Google Buzz, *infra* ¶¶ 25–30.

¹⁴ Nicholas Carlson, *WARNING: Google Buzz Has a Huge Privacy Flaw*, Silicon Alley Insider (Feb. 10, 2010), <http://www.businessinsider.com/warning-google-buzz-has-a-huge-privacy-flaw-2010-2>.

¹⁵ *Id.*

27. One Yahoo! Fellow at the Institute for the Study of Diplomacy at Georgetown University foresaw that Google Buzz could be a “tragic privacy disaster for Google, potentially of the same magnitude that Beacon was to Facebook.”¹⁶ He described the serious threats that could occur from publicly sharing a user’s Gmail contacts:

I am extremely concerned about hundreds of activists in authoritarian countries who would never want to reveal a list of their interlocutors to the outside world. Why so much secrecy? Simply because many of their contacts are other activists and often even various “democracy promoters” from Western governments and foundations. Many of those contacts would now inadvertently be made public.

....

But potential risk from disclosing such data extends far beyond just supplying authoritarian governments with better and more actionable intelligence. For example, most governments probably already suspect that some of their ardent opponents are connected to Western organizations but may lack the evidence to act on those suspicions. Now, thanks to Google's desire to make an extra buck off our data, they would finally have the ultimate proof they needed (if you think that this is unrealistic, consider this: the Iranian authorities have once used membership in an academic mailing list run out of Columbia as evidence of spying for the West).¹⁷

28. Anonymous blogger “Harriet Jacobs” described another type of threat resulting from creating automated lists from email contacts:

I use my private Gmail account to email my boyfriend and my mother.

There’s a BIG drop-off between them and my other “most frequent” contacts.

You know who my third most frequent contact is?

My abusive ex-husband.

Which is why it’s SO EXCITING, Google, that you AUTOMATICALLY allowed all my most frequent contacts access to my Reader, including all the comments I’ve made on Reader items, usually shared with my boyfriend, who

¹⁶ Evgeny Morozov, Foreign Policy Net.Effect Blog Post: *Wrong Kind of Buzz around Google Buzz* (Feb. 11, 2010), http://neteffect.foreignpolicy.com/posts/2010/02/11/wrong_kind_of_buzz_around_google_buzz.

¹⁷ *Id.*

I had NO REASON to hide my current location or workplace from, and never did.¹⁸

what did it
auto share
on Reader?

Jacobs' story received international attention and was cited in numerous articles and blog posts that discussed the privacy concerns associated with Google Buzz, including the New York Times,¹⁹ CNET,²⁰ The Telegraph,²¹ and The Guardian.²²

29. Texas lawyer Don Cruise also took issue with creating automated social networking lists from email contacts, describing Google's actions as "[r]epurposing old data in a way that flouts our expectations of privacy."²³ Cruise describes the problem this poses for professional confidentiality obligations:

There was a pretty massive shift in your privacy a couple of days ago. You might not have noticed it. But unless you take a few steps to protect yourself, Google may be sharing some of your confidences with the world.

....

Assume for just a moment that this concerns you. Assume, perhaps, that some other people might expect to be able to contact you in confidence—as a lawyer, a blogger, a journalist, or even (gasp) a friend. Assume that part of your professional responsibility is keeping the confidences of others.

Cruise offers four tips to protecting confidentiality in relationships, including the fact that “when you “turn off” Google Buzz, that doesn’t actually remove your information from search results.”²⁴ Rather, updates are hidden, although all other information is still shared.²⁵

explain?

¹⁸ Harriet Jacobs, *Fugitivus Blog Post: Fuck You Google* (Feb. 11, 2010), <http://gizmodo.com/5470696/fck-you-google>.

¹⁹ Miguel Helft, *Critics Say Google Invades Privacy with New Service*, N.Y. Times (Feb. 12, 2010), available at <http://www.nytimes.com/2010/02/13/technology/internet/13google.html>.

²⁰ Tom Krazit, *More Google Buzz Tweaks, Separate Version Coming?*, CNET News (Feb. 12, 2010), http://news.cnet.com/8301-30684_3-10453027-265.html.

²¹ Shane Richmond, *Google Buzz Tweaked after User Concerns*, Telegraph (Feb. 12, 2010), <http://blogs.telegraph.co.uk/technology/shanerichmond/100004650/google-buzz-tweaked-after-user-concerns/>.

²² Charles Arthur, *Guardian Technology Blog Post: Google Buzz's Open Approach Leads to Stalking Threat* (Feb. 12, 2010), <http://www.guardian.co.uk/technology/blog/2010/feb/12/google-buzz-stalker-privacy-problems>.

²³ Don Cruise, *The Supreme Court of Texas Blog Post: Lawyers (or Journalists) with Gmail Accounts: Careful with the Google Buzz* (Feb. 11, 2010), <http://www.scotxblog.com/legal-tech/lawyer-privacy-on-google-buzz/>.

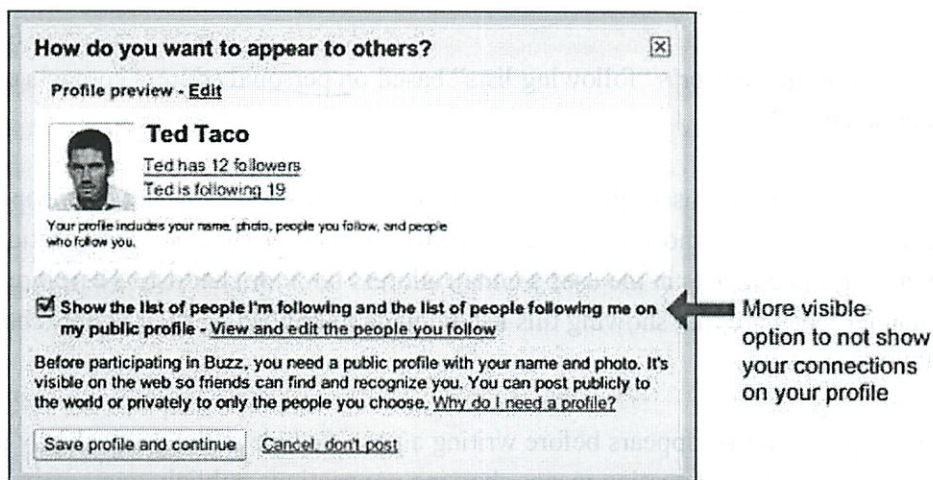
²⁴ *Id.*

²⁵ *Id.*

30. Several articles have surfaced containing information listing Buzz's privacy concerns. One such article described these three main concerns: 1) Google Buzz automatically imports contacts and shows them as friends, 2) Google Buzz grabs photos without a user uploading them, and 3) Google Buzz can pinpoint and broadcast your exact location.²⁶

First Round of Changes to Google Buzz

31. On the afternoon of February 11, 2010, in response to user criticism, Google made changes to the Google Buzz tool.²⁷
32. Google still requires users to opt out of using the Google Buzz service. When a user first clicks on the text box to write a post, a pop-up screen appears. On this screen, there is a checked box next to the option: "Show the list of people I'm following and the list of people following me on my public profile." To prevent this from occurring, a user must uncheck the box, or in other words "opt out" of sharing. For a screenshot of this window, see below.

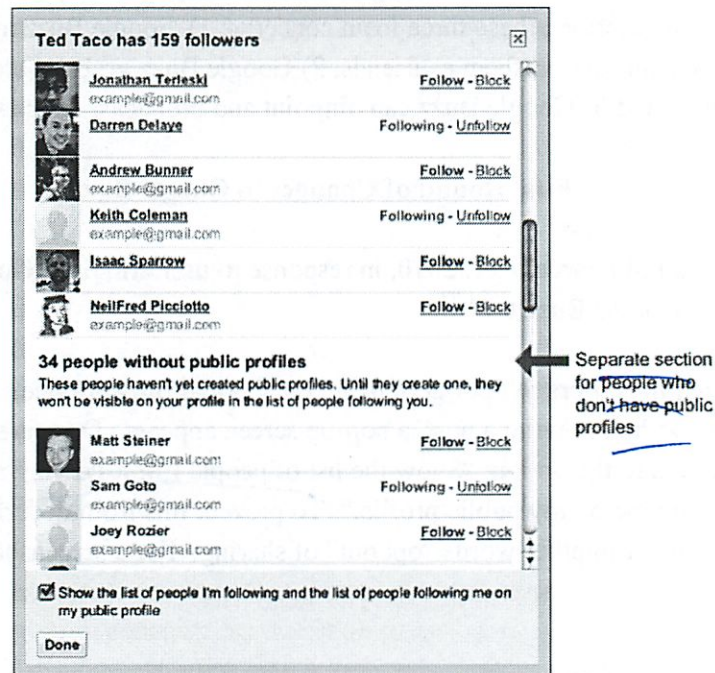


33. Google changed which of a user's connections appear on the user's public profile. Only contacts who have created a public profile will appear on a user's public follower list. Users who have not created a public profile will still be on a user's follower list, but such contacts will not be public, and cannot be seen by other contacts. For an example of this distinction, see the screenshot below:

²⁶ Andrew R. Hickey, 3 Google Buzz Privacy Concerns, ChannelWeb (Feb. 11, 2010), <http://www.crn.com/software/222900037>.

²⁷ Todd Jackson, Gmail Blog Post: Millions of Buzz Users, and Improvements Based on your Feedback (Feb. 11, 2010), <http://gmailblog.blogspot.com/2010/02/millions-of-buzz-users-and-improvements.html>.

?hidden till they post
make a notice?



34. Google still compiled a user's "following lists" based on personal address contacts and chat list contacts.
35. Google still did not notify users from the outset that Google creates the list of "people you follow" and "people who follow you" according to the frequency of conversation between a user and contacts in the user's Gmail address book or chat list. Therefore, users remained unaware that showing this list amounts to publishing their address book and Gmail contacts list.
36. On the pop-up screen that appears before writing a post, Google still did not clearly state that showing the user's connection means showing connections publicly to everyone, and having them publicly indexed by search engines. The checked box only states, "Show the list of people I'm following and the list of people following me on my profile."

Continued User Opposition to Google Buzz

37. Nicholas Carlson, with Silicon Alley Insider, observed that even with the changes, Google failed to recognize the privacy risks to normal users:

We have a message for the brilliant people behind Google Buzz (and the rest of Google's products): the rest of the world is NOT like you. These privacy

concerns aren't for the incredibly computer savvy, the patient beta testers, or Twitter and Facebook power users.²⁸

He urged Google to make the sharing of lists opt-in rather than opt-out, and to more clearly explain to users exactly what Google Buzz shares.

38. Similarly, Robin Wauters, with Tech Crunch, argued that the changes were insufficient:

Even with the improvements that were made to the Buzz product, Google is confusing the hell out of people here—and make some lives hell for them to boot.²⁹

39. CNET's Tom Krazit reported on the reaction to Google Buzz's privacy risks:

The privacy backlash certainly hurt the perception of Google and Google Buzz during the first week of the service. Those already skeptical of Google's insatiable thirst for data and its attitudes toward privacy could not help but see Google's decisions on the controls for Buzz profiles as a way of tricking people into generating public content.³⁰

He argued that Google could help address privacy concerns by adding Google Buzz to the Google Privacy Dashboard.

40. Finally, Kevin Purdy, with Lifehacker, argued that the changes fail to protect the users who had already activated Google Buzz:

Google touts in the same post the “tens of millions of people” who have logged into Buzz in some way, creating 9 million posts and comments, and those folks have to discover the non-public option on their own.³¹

²⁸ Nicholas Carlson, *Google Buzz Still Has Major Privacy Flaw*, Silicon Alley Insider, Feb. 12, 2010, <http://www.businessinsider.com/googles-nice-improvements-to-buzz-dont-correct-major-privacy-flaw-2010-2>.

²⁹ Robin Wauters, *Google Buzz Privacy Issues Have Real Life Implications*, Tech Crunch, Feb. 12, 2010, <http://www.washingtonpost.com/wp-dyn/content/article/2010/02/12/AR2010021201490.html>.

³⁰ Tom Krazit, *Google tweaks Buzz privacy settings*, CNET, Feb. 11, 2010, http://news.cnet.com/8301-30684_3-10452412-265.html.

³¹ Kevin Purdy, *Google Updates, Explains Buzz Privacy Setup*, Lifehacker, Feb. 11, 2010, <http://lifehacker.com/5470104/google-updates-explains-buzz-privacy-setup>.

























Google Buzz's Second Round of Changes

41. On February 13, 2010, in response to continued user criticism, Google made more changes to Google Buzz in an effort to address privacy concerns.³²
42. Google is now using an auto-suggest model, rather than an auto-follow model. In other words, "You won't be set up to follow anyone until you have reviewed the suggestions and clicked 'Follow selected people and start using Buzz.'"³³ For a screenshot of the new welcome page for Google Buzz, see below.³⁴

Welcome to Google Buzz

Follow your friends to get started
In Buzz, you'll see posts from the people you follow. Here are some suggestions to get started, based on the people you email and chat with the most. You can find more people to follow later. [Learn more](#)

Select: All None

<input checked="" type="checkbox"/>  Ed Ho example@gmail.com	<input checked="" type="checkbox"/>  Ken Norton example@gmail.com	<input checked="" type="checkbox"/>  Braden Kowitz example@gmail.com
<input checked="" type="checkbox"/>  Arielle Reinstein example@gmail.com	<input checked="" type="checkbox"/>  Matt Steiner example@gmail.com	<input checked="" type="checkbox"/>  Sam Goto example@gmail.com
<input checked="" type="checkbox"/>  Brian Stoler example@gmail.com	<input checked="" type="checkbox"/>  Bruce DiBello example@gmail.com	<input checked="" type="checkbox"/>  Henry Wong example@gmail.com
<input checked="" type="checkbox"/>  Keith Coleman example@gmail.com	<input checked="" type="checkbox"/>  Joey Rozier example@gmail.com	<input checked="" type="checkbox"/>  Grace Kwaak example@gmail.com
<input checked="" type="checkbox"/>  Bradley Horowitz example@gmail.com	<input checked="" type="checkbox"/>  Matt Waddell example@gmail.com	<input checked="" type="checkbox"/>  Andrew Bunner example@gmail.com
<input checked="" type="checkbox"/>  Sam Schillace example@gmail.com	<input checked="" type="checkbox"/>  Niranjan Tulpule example@gmail.com	<input checked="" type="checkbox"/>  Steve Crossan example@gmail.com
<input checked="" type="checkbox"/>  Sean McBride example@gmail.com	<input checked="" type="checkbox"/>  Dave Cohen example@gmail.com	<input checked="" type="checkbox"/>  Jake Knapp example@gmail.com
<input checked="" type="checkbox"/>  Punit Soni example@gmail.com	<input checked="" type="checkbox"/>  Jeff Huber example@gmail.com	<input checked="" type="checkbox"/>  Michael Leggett example@gmail.com

The first time you post in Buzz you'll create a profile which includes the list of people you follow -- you can choose not to display this list if you'd like.

Follow selected people and start using Buzz Turn off Buzz

43. Google Buzz still populates the suggested social networking list of people a user follows based on frequent address book and chat contacts. Although the "welcome page" states that "[y]ou can find more people to follow later," the contacts from a user's address book and chat list make up a user's initial "follow" list.

well pre checked box will hit better

³² Todd Jackson, Google Blog Post: *A New Buzz Start-up Experience Based on your Feedback* (Feb. 13, 2010), <http://gmailblog.blogspot.com/2010/02/new-buzz-start-up-experience-based-on.html>.

³³ *Id.*

³⁴ *Id.*

I think this is done

44. Google Buzz still allows people to automatically follow a user. The burden remains on the user to block those unwanted followers. As a CNET article explained, “It will give those who acquiesced to Google’s sleight of software another chance to review those automatically chosen to be followed, just to check whether there might some unwanted ex-husbands, ex-girlfriends, or slightly insane stalkers that slipped through the net.”³⁵
45. The “welcome screen” does not make clear that the user must create a profile that would be public and indexed by search engines. The screen only states, “The first time you post in Buzz you’ll create a profile which includes the list of people you follow—you can choose not to display this list if you’d like.”
46. Google has not announced any changes to the pop-up screen that appears when a user initially posts on Google Buzz. Users are still unaware that showing the user’s connection means showing connections publicly to everyone, and having them publicly indexed by search engines.

III. Legal Analysis

The FTC’s Section 5 Authority

47. Google is engaging in unfair and deceptive acts and practices.³⁶ Such practices are prohibited by the FTC Act, and the Commission is empowered to enforce the Act’s prohibitions.³⁷ These powers are described in FTC Policy Statements on Deception³⁸ and Unfairness.³⁹
48. A trade practice is unfair if it “causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.”⁴⁰

³⁵ Chris Matyszczyk, *Google Changes Buzz Privacy Settings – Again*, CNET News (Feb. 14, 2010), http://news.cnet.com/8301-17852_3-10453274-71.html.

³⁶ See 15 U.S.C. § 45.

³⁷ *Id.*

³⁸ Fed. Trade Comm’n, FTC Policy Statement on Deception (1983), *available at* <http://www.ftc.gov/bcp/policystmt/ad-decept.htm> [*hereinafter* FTC Deception Policy].

³⁹ Fed. Trade Comm’n, FTC Policy Statement on Unfairness (1980), *available at* <http://www.ftc.gov/bcp/policystmt/ad-unfair.htm> [*hereinafter* FTC Unfairness Policy].

⁴⁰ 15 U.S.C. § 45(n); *see, e.g., Fed. Trade Comm’n v. Seismic Entertainment Productions, Inc.*, Civ. No. 1:04-CV-00377 (Nov. 21, 2006) (finding that unauthorized changes to users’ computers that affected the functionality of the computers as a result of Seismic’s anti-spyware software constituted a “substantial injury without countervailing benefits.”).

49. The injury must be “substantial.”⁴¹ Typically, this involves monetary harm, but may also include “unwarranted health and safety risks.”⁴² Emotional harm and other “more subjective types of harm” generally do not make a practice unfair.⁴³ Secondly, the injury “must not be outweighed by an offsetting consumer or competitive benefit that the sales practice also produces.”⁴⁴ Thus the FTC will not find a practice unfair “unless it is injurious in its net effects.”⁴⁵ Finally, “the injury must be one which consumers could not reasonably have avoided.”⁴⁶ This factor is an effort to ensure that consumer decision making still governs the market by limiting the FTC to act in situations where seller behavior “unreasonably creates or takes advantage of an obstacle to the free exercise of consumer decisionmaking.”⁴⁷ Sellers may not withhold from consumers important price or performance information, engage in coercion, or unduly influence highly susceptible classes of consumers.⁴⁸

50. The FTC will also look at “whether the conduct violates public policy as it has been established by statute, common law, industry practice, or otherwise.”⁴⁹ Public policy is used to “test the validity and strength of the evidence of consumer injury, or, less often, it may be cited for a dispositive legislative or judicial determination that such injury is present.”⁵⁰

51. The FTC will make a finding of deception if there has been a “representation, omission or practice that is likely to mislead the consumer acting reasonably in the circumstances, to the consumer’s detriment.”⁵¹

52. First, there must be a representation, omission, or practice that is likely to mislead the consumer.⁵² The relevant inquiry for this factor is not whether the act or practice actually

⁴¹ FTC Unfairness Policy, *supra* note 113.

⁴² *Id.*; see, e.g., *Fed. Trade Comm’n v. Information Search, Inc.*, Civ. No. 1:06-cv-01099 (Mar. 9, 2007) (“The invasion of privacy and security resulting from obtaining and selling confidential customer phone records without the consumers’ authorization causes substantial harm to consumers and the public, including, but not limited to, endangering the health and safety of consumers.”).

⁴³ FTC Unfairness Policy, *supra* note 113.

⁴⁴ *Id.*

⁴⁵ *Id.*

⁴⁶ *Id.*

⁴⁷ *Id.*

⁴⁸ *Id.*

⁴⁹ *Id.*

⁵⁰ *Id.*

⁵¹ FTC Deception Policy, *supra* note 112.

⁵² FTC Deception Policy, *supra* note 112; see, e.g., *Fed Trade Comm’n v. Pantron I Corp.*, 33 F.3d 1088 (9th Cir. 1994) (holding that Pantron’s representation to consumers that a product was effective at reducing hair loss was materially misleading, because according to studies, the success of the product could only be attributed to a placebo effect, rather than on scientific grounds).

misled the consumer, but rather whether it is likely to mislead.⁵³ Second, the act or practice must be considered from the perspective of a reasonable consumer.⁵⁴ “The test is whether the consumer’s interpretation or reaction is reasonable.”⁵⁵ The FTC will look at the totality of the act or practice and ask questions such as “how clear is the representation? How conspicuous is any qualifying information? How important is the omitted information? Do other sources for the omitted information exist? How familiar is the public with the product or service?”⁵⁶

53. Finally, the representation, omission, or practice must be material.⁵⁷ Essentially, the information must be important to consumers. The relevant question is whether consumers would have chosen another product if the deception had not occurred.⁵⁸ Express claims will be presumed material.⁵⁹ Materiality is presumed for claims and omissions involving “health, safety, or other areas with which the reasonable consumer would be concerned.”⁶⁰ The harms of this social networking site’s practices are within the scope of the FTC’s authority to enforce Section 5 of the FTC Act and its purveyors should face FTC action for these violations.

IV. Prayer for Investigation and Relief

54. EPIC requests that the Commission investigate Google, enjoin its unfair and deceptive business practices, and require Google to protect the privacy of Gmail users. Specifically, EPIC requests the Commission to:

Compel Google to make Google Buzz a fully opt-in service for Gmail users;

Compel Google to cease using Gmail users’ private address book contacts to compile social networking lists;

Compel Google to give Google Buzz users more control over their information, by allowing users to accept or reject followers from the outset; and

Provide such other relief as the Commission finds necessary and appropriate.

⁵³ FTC Deception Policy, *supra* note 112.

⁵⁴ *Id.*

⁵⁵ *Id.*

⁵⁶ *Id.*

⁵⁷ *Id.*

⁵⁸ *Id.*

⁵⁹ *Id.*

⁶⁰ *Id.*

55. EPIC reserves the right to supplement this petition as other information relevant to this proceeding becomes available.

Respectfully Submitted,

Marc Rotenberg, EPIC Executive Director

Kimberly Nguyen, EPIC Consumer Privacy Counsel

Jared Kaprove, EPIC Domestic Surveillance Counsel

ELECTRONIC PRIVACY INFORMATION CENTER

1718 Connecticut Ave., NW Suite 200

Washington, DC 20009

202-483-1140 (tel)

202-483-1248 (fax)

Reud 11/3

102 3136

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION

COMMISSIONERS: Jon Leibowitz, Chairman
William E. Kovacic
J. Thomas Rosch
Edith Ramirez
Julie Brill

In the Matter of

GOOGLE INC.,
a corporation.

DOCKET NO.

COMPLAINT

The Federal Trade Commission, having reason to believe that Google Inc. ("Google" or "respondent"), a corporation, has violated the Federal Trade Commission Act ("FTC Act"), and it appearing to the Commission that this proceeding is in the public interest, alleges:

1. Respondent Google is a Delaware corporation with its principal office or place of business at 1600 Amphitheatre Parkway, Mountain View, CA 94043.
2. The acts and practices of respondent as alleged in this complaint have been in or affecting commerce, as "commerce" is defined in Section 4 of the FTC Act.

RESPONDENT'S BUSINESS PRACTICES

3. Google is a technology company best known for its web-based search engine, which provides free search results to consumers. Google also provides various free web products to consumers, including its widely used web-based email service, Gmail, which has been available since April 2004. Among other things, Gmail allows consumers to send and receive emails, chat with other users through Google's instant messaging service, Google Chat, and store email messages, contact lists, and other information on Google's servers.
4. Google's free web products for consumers also include: Google Reader, which allows users to subscribe to, read, and share content online; Picasa, which allows users to edit, post, and share digital photos; and Blogger, Google's weblog publishing tool that allows users to share text, photos, and video.
5. Google also offers consumers the ability to create a "Google profile," which enables

them to make certain information about themselves public and to link to their content on Google product websites, such as the user's Google Reader shared items, public Picasa Web Albums, and Blogger blog. Information on a consumer's public Google profile, which may include the consumer's name, location, and photo, is available on the Internet and may be indexed by search engines.

RESPONDENT'S STATEMENTS

6. Respondent has disseminated or caused to be disseminated statements to consumers on its website regarding its privacy practices, including but not limited to:
 - a. From approximately October 2004 until October 2010, the following statement in the Gmail Privacy Policy about Google's use of consumer information provided through Gmail:

Gmail stores, processes and maintains your messages, contact lists and other data related to your account in order to provide the service to you.
 - b. From approximately October 2005 until October 2010, the following statement in Google's Privacy Policy regarding consumers' choices about the uses of their personal information in all of Google's products, including Gmail:

When you sign up for a particular service that requires registration, we ask you to provide personal information. If we use this information in a manner different than the purpose for which it was collected, then we will ask for your consent prior to such use.

RESPONDENT'S LAUNCH OF GOOGLE BUZZ

7. On February 9, 2010, Google launched a social networking service called Google Buzz ("Google Buzz" or "Buzz") within the Gmail product. Google Buzz is a platform that allows users to share updates, comments, photos, videos, and other information through posts or "buzzes" made either publicly or privately to individuals or groups of users. Google used the information of consumers who signed up for Gmail, including first and last name and email contacts, to populate the social network. Without prior notice or the opportunity to consent, Gmail users were, in many instances, automatically set up with "followers" (people following the user). In addition, after enrolling in Buzz, Gmail users were automatically set up to "follow" other users.
8. On the day Buzz was launched, Gmail users who signed into their accounts were taken to a welcome screen that announced the new service and highlighted features such as: "No set up needed – You're already following the people you email and chat with the most in Gmail." Gmail users had to elect one of two options to proceed to their inboxes: "Sweet!

Check out Buzz” or “Nah, go to my inbox.” **Exhibit A** shows how the initial Buzz screen appeared to consumers.

- a. If a Gmail user selected “Nah, go to my inbox” from the initial Buzz screen, that user’s information was nonetheless shared in a number of ways:
 - i. The user could be “followed” by other Gmail users who had enrolled in Buzz.
 - ii. If the user had previously created a public Google profile, the user could appear on the public Google profiles of people who had enrolled in Buzz and were following the user.
 - iii. A Buzz link would appear in the list of links on the user’s Gmail page. If the user clicked on the that link, he or she would be taken to the Buzz welcome screen and automatically enrolled in Buzz, without any disclosure of that fact and without any further action on the user’s part. **Exhibit B** shows how the Buzz welcome screen appeared to consumers. The user would be enrolled in Buzz even if the user did not click the “Okay” button at the bottom of the welcome screen.
 - b. Regardless of whether they chose “Sweet! Check out Buzz” or “Nah, go to my inbox,” Gmail users had an option to click a “Turn off Buzz” link, contained in small type at the bottom of the Gmail home page after login. Clicking that link removed the Buzz tab from the user’s Gmail page. Gmail users who had clicked “Sweet! Check out Buzz” or had clicked on the Buzz link in Gmail, then later clicked the “Turn off Buzz” link, nonetheless continued to appear as a “follower” on the Google profiles and Google Buzz pages of the people whom they emailed the most. In addition, on each such profile, a “follow” link was placed next to the Gmail user’s name, so other individuals could begin following the user.
9. The setup process for Gmail users who enrolled in Buzz did not adequately communicate that certain previously private information would be shared publicly by default. Further, the controls that would allow the user to change the defaults were confusing and difficult to find.
- a. Users who clicked on “Sweet! Check out Buzz” from the Buzz welcome screen, as well as users that selected “Nah, go to my Inbox” and later clicked the Buzz tab, were directed to a Buzz welcome screen that stated: “You’re set up to follow the people you email and chat with the most,” and listed the users’ followers and the people the user was set up to follow. However, there was no disclosure on this screen that, by default, those lists might later be posted on a user’s public Google profile, exposing the list of people with whom a user chatted or emailed most often. *See Exhibit B.*

- b. When first attempting to post in Buzz, users were directed to click through a profile creation screen, which explained that users needed to create a public Google profile before participating in Buzz. The profile creation screen contained the following header: “How do you want to appear to others?” The screen also included the following language in prominent, contrasting type: “Before participating in Buzz, you need a public profile with your name and photo. It’s visible on the web so friends can find and recognize you. You can post publicly to the world or privately to only the people you choose.” The profile creation screen also included the following language in small gray letters against a white background: “Your profile will include your name, photo, people you follow and people who follow you.” **Exhibit C** shows how the profile creation screen appeared to consumers.
 - c. In order to find controls that would allow the user to stop following certain individuals, a user had to take the additional step to click a link marked “edit,” which expanded the profile creation screen. Only after clicking “edit” could users choose not to have their lists of followers and people the user was following shown on the user’s public Google profile. They did so by unchecking a pre-checked box. Users who saw no reason to edit their profile – particularly those who already had created a Google profile and did not realize new information would be added and publicly available by default on that profile – would never have learned that these controls were available. **Exhibit D** shows how the expanded profile creation screen appeared to consumers.
 - d. The default setting for items posted in Google Buzz was “public” – shared with all of a user’s followers – though users had the ability to select “private” from a drop-down menu to post to a more limited group. Public buzzes were added to a user’s public Google profile, which was searchable on the Internet and could be indexed by search engines.
 - e. Google Buzz also automatically connected to other information users had made public through Google products such as Picasa and Reader. In many instances, this information was automatically compiled and broadcast in public buzzes that showed up on the user’s public Google profile.
10. Certain personal information of Gmail users was shared without consumers’ permission through the Google Buzz social network.
- a. In some cases, Gmail users had previously blocked certain email contacts from viewing other information about them, but those preferences were not carried over to Buzz. For example, even if a Gmail user blocked an individual in Google Chat or Google Reader, that person was not blocked in Buzz and could show up as a follower of that Gmail user.

- b. Users could not block followers who did not have a public Google profile. Moreover, an individual who had not provided a first or last name when setting up a Google account would appear as an “unknown” follower to a user. The user was not only unable to block such an individual from following them, but they had no way of knowing the individual’s identity.
 - c. If a Google Buzz user wanted to reply or direct a comment to an individual, the user placed the @ sign in front of the individual’s name, and Google suggested names from a user’s contact list. If the user selected a name or account from the suggest list that was not associated with a Google profile, Buzz filled in the field with that person’s private email address. Using an individual’s private email address in a public reply or comment thus exposed the address to all followers of the user and allowed that email address to be accessed by search engines.
11. In response to the launch of Google Buzz, many users complained about the automatic generation of lists of followers and people to follow from email contact lists that included in some cases: individuals against whom they had obtained restraining orders; abusive ex-husbands; clients of mental health professionals; clients of attorneys; children; and recruiters they had emailed regarding job leads. Further, because of the default settings and the complex and multi-step nature of respondent’s disclosures described in **paragraph 9**, consumers were confused about what information was made public through Buzz and complained about the potential disclosure of private email addresses.
12. Following widespread public criticism and thousands of consumer complaints, Google made certain changes to the Buzz service. Among other things, Google: (1) gave users the ability to effectively disable or turn off Buzz; (2) switched from setting up Gmail users with an automatic list of people to follow to suggesting a list of people to follow for users to approve; (3) made the process for editing lists of followers and people to follow clearer and more easily accessible; (4) made it possible for users to block any follower, regardless of whether that follower had a public profile; (5) made the option not to show lists of followers on a user’s public profile more prominent; (6) discontinued the feature that automatically connected to information from other websites, such as Picasa and Google Reader; and (7) fixed the @ reply function so that private email addresses of users would not be made public.

VIOLATIONS OF THE FTC ACT

13. As set forth in **paragraph 6(a)**, respondent has represented, expressly or by implication, that it used, and would use, information from consumers signing up for Gmail only for the purpose of providing them with a web-based email service.
14. In truth and in fact, as described in **paragraphs 7-11**, respondent did not use information from consumers signing up for Gmail only for the purpose of providing them with a web-based email service. Instead, Google used this information to populate its new social

networking service. Therefore, the representations set forth in **paragraph 13** were, and are, false or misleading and constitute a deceptive act or practice.

15. As set forth in **paragraph 6(b)**, respondent has represented, expressly or by implication, that it would seek consumers' consent to use information they provided for a purpose other than that for which it was collected.
16. In truth and in fact, as described in **paragraphs 7-11**, respondent did not seek consumers' consent before using the information they provided in connection with Gmail for the Google Buzz social networking product. Therefore, the representations set forth in **paragraph 15** were, and are, false or misleading and constitute a deceptive act or practice.
17. As set forth in **paragraph 8**, by offering the option "Nah, go to my inbox," as well as the option to "Turn off Buzz," respondent has represented, expressly or by implication, that consumers who clicked on these options would not be enrolled in Buzz.
18. In truth and in fact, as described in **paragraph 8**, consumers who clicked on these options were enrolled in certain features of Buzz. Therefore, the representations set forth in **paragraph 17** were, and are, false and misleading and constitute a deceptive act or practice.
19. As set forth in **paragraph 9**, respondent represented, expressly or by implication, through the Buzz enrollment screens and statements such as "How do you want to appear to others?" that consumers would be able to exercise control over what information would be made public through their Google public profile. Respondent failed to disclose, or failed to disclose adequately, that in most instances the contacts with whom users emailed and chatted the most would become public by default and that user information submitted through other Google products would be automatically broadcast through Buzz. These facts would be material to consumers in their enrollment in and use of the Google Buzz service. Therefore, respondent's failure to adequately disclose these facts, in light of the representations made, was, and is, a deceptive act or practice.

U.S.-EU SAFE HARBOR FRAMEWORK

20. The U.S.-EU Safe Harbor Framework provides a method for U.S. companies to transfer personal data outside of the European Union ("EU") that is consistent with the requirements of the European Union Data Protection Directive ("Directive"). The Directive sets forth EU requirements for privacy and the protection of personal data. Among other things, it requires EU Member States to implement legislation that prohibits the transfer of personal data outside the EU, with exceptions, unless the European Commission ("EC") has made a determination that the recipient jurisdiction's laws ensure the protection of such personal data. This determination is commonly referred to as meeting the EU's "adequacy" standard.

21. To satisfy the EU's adequacy standard for certain commercial transfers, the U.S. Department of Commerce ("Commerce") and the EC negotiated the U.S.-EU Safe Harbor Framework, which went into effect in 2000. The Safe Harbor is a voluntary framework that allows U.S. companies to transfer personal data lawfully from the EU to the U.S. To join the Safe Harbor, a company must self-certify to Commerce that it complies with seven principles and related requirements that have been deemed to meet the EU's adequacy standard.
22. The Safe Harbor privacy principles, issued by Commerce on July 21, 2000, include the following:

NOTICE: An organization must inform individuals about the purposes for which it collects and uses information about them, how to contact the organization with any inquiries or complaints, the types of third parties to which it discloses the information, and the choices and means the organization offers individuals for limiting its use and disclosure. This notice must be provided in clear and conspicuous language when individuals are first asked to provide personal information to the organization or as soon thereafter as is practicable, but in any event before the organization uses such information for a purpose other than that for which it was originally collected or processed by the transferring organization or discloses it for the first time to a third party.

CHOICE: An organization must offer individuals the opportunity to choose (opt out) whether their personal information is (a) to be disclosed to a third party or (b) to be used for a purpose that is incompatible with the purpose(s) for which it was originally collected or subsequently authorized by the individual. Individuals must be provided with clear and conspicuous, readily available, and affordable mechanisms to exercise choice.

23. From October 2005 until the present, Google has maintained a current self-certification to Commerce and has appeared on the list of Safe Harbor companies on the Commerce website. Prior to the launch of the Buzz social networking product, Google transferred data collected from Gmail users in Europe to the United States for processing.
24. From approximately October 2005 until the present, Google made the following statement in its Privacy Policy regarding its participation in the U.S.-EU Safe Harbor Framework:

Google adheres to the US Safe Harbor Privacy Principles of Notice, Choice, Onward Transfer, Security, Data Integrity, Access and Enforcement, and is registered with the U.S. Department of Commerce's Safe Harbor Program.

25. In truth and in fact, as described in **paragraph 7**, respondent did not adhere to the US Safe Harbor Privacy Principles of Notice and Choice. In particular, respondent did not give Gmail users notice before using the information collected for Gmail for a purpose

other than that for which it was originally collected. Respondent also did not give Gmail users choice about using their information for a purpose that was incompatible with the purpose for which it was originally collected. Therefore, the representations set forth in **paragraphs 23 and 24** were, and are, false or misleading and constitutes a deceptive act or practice.

26. The acts and practices of respondent as alleged in this complaint constitute unfair or deceptive acts or practices, in or affecting commerce, in violation of Section 5(a) of the Federal Trade Commission Act.

THEREFORE, the Federal Trade Commission this ____ day of _____, 2011, has issued this complaint against respondent.

By the Commission.

Donald S. Clark
Secretary

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION

File No. 102 3136

In the Matter of

GOOGLE INC.,
a corporation.

)
)
)
)
)
)
)
**AGREEMENT CONTAINING
CONSENT ORDER**

The Federal Trade Commission has conducted an investigation of certain acts and practices of Google Inc. ("Google" or "proposed respondent"). Google, having been represented by counsel, is willing to enter into an agreement containing a consent order resolving the allegations contained in the attached draft complaint. Therefore,

IT IS HEREBY AGREED by and between Google, by its duly authorized officials, and counsel for the Federal Trade Commission that:

1. Proposed respondent Google is a Delaware corporation with its principal office or place of business at 1600 Amphitheatre Parkway, Mountain View, CA 94043.
2. Proposed respondent admits all the jurisdictional facts set forth in the draft complaint.
3. Proposed respondent waives:
 - A. any further procedural steps;
 - B. the requirement that the Commission's decision contain a statement of findings of fact and conclusions of law; and
 - C. all rights to seek judicial review or otherwise to challenge or contest the validity of the order entered pursuant to this agreement.
4. This agreement shall not become part of the public record of the proceeding unless and until it is accepted by the Commission. If this agreement is accepted by the Commission, it, together with the draft complaint, will be placed on the public record for a period of thirty (30) days and information about it publicly released. The Commission thereafter may either withdraw its acceptance of this agreement and so notify proposed respondent, in which event it will take such action as it may consider appropriate, or issue and serve its complaint (in such form as the circumstances may require) and decision in disposition of the proceeding.

5. This agreement is for settlement purposes only and does not constitute an admission by proposed respondent that the law has been violated as alleged in the draft complaint, or that the facts as alleged in the draft complaint, other than the jurisdictional facts, are true.
6. This agreement contemplates that, if it is accepted by the Commission, and if such acceptance is not subsequently withdrawn by the Commission pursuant to the provisions of Section 2.34 of the Commission's Rules, the Commission may, without further notice to proposed respondent, (1) issue its complaint corresponding in form and substance with the attached draft complaint and its decision containing the following order in disposition of the proceeding, and (2) make information about it public. When so entered, the order shall have the same force and effect and may be altered, modified, or set aside in the same manner and within the same time provided by statute for other orders. The order shall become final upon service. Delivery of the complaint and the decision and order to proposed respondent's address, as provided to the Commission by the proposed respondent, by any means specified in Section 4.4(a) of the Commission's Rules, shall constitute service. Proposed respondent waives any right he may have to any other manner of service. The complaint may be used in construing the terms of the order. No agreement, understanding, representation, or interpretation not contained in the order or the agreement may be used to vary or contradict the terms of the order.
7. Proposed respondent has read the draft complaint and consent order. Proposed respondent understands that it may be liable for civil penalties in the amount provided by law and other appropriate relief for each violation of the order after it becomes final.

ORDER

DEFINITIONS

For purposes of this order, the following definitions shall apply:

1. Unless otherwise specified, "respondent" shall mean Google, its successors and assigns, officers, agents, representatives, and employees. For the purpose of Parts I, II, and III of this order, "respondent" shall also mean Google acting directly or through any corporation, subsidiary, division, website, or other device.
2. "Clear(ly) and prominent(ly)" shall mean:
 - A. In textual communications (e.g., printed publications or words displayed on the screen of a computer or mobile device), the required disclosures are of a type, size, and location sufficiently noticeable for an ordinary consumer to read and comprehend them, in print that contrasts highly with the background on which they appear;

- B. In communications disseminated orally or through audible means (e.g., radio or streaming audio), the required disclosures are delivered in a volume and cadence sufficient for an ordinary consumer to hear and comprehend them;
 - C. In communications disseminated through video means (e.g., television or streaming video), the required disclosures are in writing in a form consistent with subpart (A) of this definition and shall appear on the screen for a duration sufficient for an ordinary consumer to read and comprehend them, and in the same language as the predominant language that is used in the communication; and
 - D. In all instances, the required disclosures: (1) are presented in an understandable language and syntax; and (2) include nothing contrary to, inconsistent with, or in mitigation of any other statements or disclosures provided by respondent.
- 3. "Commerce" shall mean as defined in Section 4 of the Federal Trade Commission Act, 15 U.S.C. § 44.
 - 4. "Google user" shall mean an identified individual from whom respondent has collected information for the purpose of providing access to respondent's products and services.
 - 5. "Covered information" shall mean information respondent collects from or about an individual, including, but not limited to, an individual's: (a) first and last name; (b) home or other physical address, including street name and city or town; (c) email address or other online contact information, such as a user identifier or screen name; (d) persistent identifier, such as IP address; (e) telephone number, including home telephone number and mobile telephone number; (f) list of contacts; (g) physical location; or any other information from or about an individual consumer that is combined with (a) through (g) above.
 - 6. "Third party" shall mean any individual or entity other than: (1) respondent; (2) a service provider of respondent that: (i) uses or receives covered information collected by or on behalf of respondent for and at the direction of the respondent and no other individual or entity, (ii) does not disclose the data, or any individually identifiable information derived from such data, to any individual or entity other than respondent, and (iii) does not use the data for any other purpose; or (3) any entity that uses covered information only as reasonably necessary: (i) to comply with applicable law, regulation, or legal process, (ii) to enforce respondent's terms of use, or (iii) to detect, prevent, or mitigate fraud or security vulnerabilities.

I.

IT IS ORDERED that respondent, in or affecting commerce, shall not misrepresent in any manner, expressly or by implication:

- A. the extent to which respondent maintains and protects the privacy and confidentiality of any covered information, including, but not limited to, misrepresentations related to: (1) the purposes for which it collects and uses covered information, and (2) the extent to which consumers may exercise control over the collection, use, or disclosure of covered information.
- B. the extent to which respondent is a member of, adheres to, complies with, is certified by, is endorsed by, or otherwise participates in any privacy, security, or any other compliance program sponsored by the government or any other entity, including, but not limited to, the U.S.-EU Safe Harbor Framework.

II.

IT IS FURTHER ORDERED that respondent, prior to any new or additional sharing by respondent of the Google user's identified information with any third party, that: 1) is a change from stated sharing practices in effect at the time respondent collected such information, and 2) results from any change, addition, or enhancement to a product or service by respondent, in or affecting commerce, shall:

- A. Separate and apart from any final "end user license agreement," "privacy policy," "terms of use" page, or similar document, clearly and prominently disclose: (1) that the Google user's information will be disclosed to one or more third parties, (2) the identity or specific categories of such third parties, and (3) the purpose(s) for respondent's sharing; and
- B. Obtain express affirmative consent from the Google user to such sharing.

III.

IT IS FURTHER ORDERED that respondent, in or affecting commerce, shall, no later than the date of service of this order, establish and implement, and thereafter maintain, a comprehensive privacy program that is reasonably designed to: (1) address privacy risks related to the development and management of new and existing products and services for consumers, and (2) protect the privacy and confidentiality of covered information. Such program, the content and implementation of which must be documented in writing, shall contain privacy controls and procedures appropriate to respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the covered information, including:

- A. the designation of an employee or employees to coordinate and be responsible for the privacy program.
- B. the identification of reasonably foreseeable, material risks, both internal and external, that could result in the respondent's unauthorized collection, use, or disclosure of covered information, and an assessment of the sufficiency of any safeguards in place to control these risks. At a minimum, this privacy risk

Privacy
Cler

assessment should include consideration of risks in each area of relevant operation, including, but not limited to: (1) employee training and management, including training on the requirements of this order, and (2) product design, development, and research.

- C. the design and implementation of reasonable privacy controls and procedures to address the risks identified through the privacy risk assessment, and regular testing or monitoring of the effectiveness of those privacy controls and procedures.
- D. the development and use of reasonable steps to select and retain service providers capable of appropriately protecting the privacy of covered information they receive from respondent, and requiring service providers by contract to implement and maintain appropriate privacy protections.
- E. the evaluation and adjustment of respondent's privacy program in light of the results of the testing and monitoring required by subpart C, any material changes to respondent's operations or business arrangements, or any other circumstances that respondent knows or has reason to know may have a material impact on the effectiveness of its privacy program.

IV.

IT IS FURTHER ORDERED that, in connection with its compliance with Part III of this order, respondent shall obtain initial and biennial assessments and reports ("Assessments") from a qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession. A person qualified to prepare such Assessments shall have a minimum of three (3) years of experience in the field of privacy and data protection. All persons conducting such Assessments and preparing such reports shall be approved by the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580, in his or her sole discretion. The reporting period for the Assessments shall cover: (1) the first one hundred and eighty (180) days after service of the order for the initial Assessment, and (2) each two (2) year period thereafter for twenty (20) years after service of the order for the biennial Assessments. Each Assessment shall:

- A. set forth the specific privacy controls that respondent has implemented and maintained during the reporting period;
- B. explain how such privacy controls are appropriate to respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the covered information;
- C. explain how the privacy controls that have been implemented meet or exceed the protections required by Part III of this order; and

- D. certify that the privacy controls are operating with sufficient effectiveness to provide reasonable assurance to protect the privacy of covered information and that the controls have so operated throughout the reporting period.

Each Assessment shall be prepared and completed within sixty (60) days after the end of the reporting period to which the Assessment applies. Respondent shall provide the initial Assessment to the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580, within ten (10) days after the Assessment has been prepared. All subsequent biennial Assessments shall be retained by respondent until the order is terminated and provided to the Associate Director of Enforcement within ten (10) days of request.

V.

IT IS FURTHER ORDERED that respondent shall maintain and upon request make available to the Federal Trade Commission for inspection and copying, unless respondent asserts a valid legal privilege, a print or electronic copy of:

- A. for a period of three (3) years from the date of preparation or dissemination, whichever is later, all widely disseminated statements that describe the extent to which respondent maintains and protects the privacy and confidentiality of any covered information, with all materials relied upon in making or disseminating such statements;
- B. for a period of six (6) months from the date received, all consumer complaints directed at respondent, or forwarded to respondent by a third party, that allege unauthorized collection, use, or disclosure of covered information and any responses to such complaints;
- C. for a period of five (5) years from the date received, any documents, whether prepared by or on behalf of respondent, that contradict, qualify, or call into question respondent's compliance with this order; and
- D. for a period of three (3) years after the date of preparation of each Assessment required under Part III of this order, all materials relied upon to prepare the Assessment, whether prepared by or on behalf of respondent, including but not limited to all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, for the compliance period covered by such Assessment.

VI.

IT IS FURTHER ORDERED that respondent shall deliver a copy of this order to all current and future principals, officers, directors, and managers, and to all current and future employees, agents, and representatives having supervisory responsibilities relating to the subject

matter of this order. Respondent shall deliver this order to such current personnel within thirty (30) days after service of this order, and to such future personnel within thirty (30) days after the person assumes such position or responsibilities.

VII.

IT IS FURTHER ORDERED that respondent shall notify the Commission at least thirty (30) days prior to any change in the corporation that may affect compliance obligations arising under this order, including, but not limited to, a dissolution, assignment, sale, merger, or other action that would result in the emergence of a successor corporation; the creation or dissolution of a subsidiary, parent, or affiliate that engages in any acts or practices subject to this order; the proposed filing of a bankruptcy petition; or a change in either corporate name or address. Provided, however, that, with respect to any proposed change in the corporation about which respondent learns less than thirty (30) days prior to the date such action is to take place, respondent shall notify the Commission as soon as is practicable after obtaining such knowledge. All notices required by this Part shall be sent by certified mail to the Associate Director, Division of Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580.

VIII.

IT IS FURTHER ORDERED that respondent shall, within ninety (90) days after the date of service of this order file with the Commission a true and accurate report, in writing, setting forth in detail the manner and form in which respondent has complied with this order. Within ten (10) days of receipt of written notice from a representative of the Commission, respondent shall submit additional true and accurate written reports.

IX.

This order will terminate twenty (20) years from the date of its issuance, or twenty (20) years from the most recent date that the United States or the Commission files a complaint (with or without an accompanying consent decree) in federal court alleging any violation of the order, whichever comes later; provided, however, that the filing of such a complaint will not affect the duration of:

- A. any Part in this order that terminates in fewer than twenty (20) years;
- B. this order if such complaint is filed after the order has terminated pursuant to this Part.

Provided, further, that if such complaint is dismissed or a federal court rules that respondent did not violate any provision of the order, and the dismissal or ruling is either not appealed or upheld on appeal, then the order as to such respondent will terminate according to this Part as though the complaint had never been filed, except that the order will not terminate between the date

such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

Signed this _____ day of _____, 2011.

GOOGLE INC.

By: _____

ALBERT GIDARI
Perkins Coie
Counsel for Google Inc.

KENT WALKER
Senior Vice President & General
Counsel
Google Inc.

FEDERAL TRADE COMMISSION

By: _____

KATHRYN D. RATTÉ
Counsel for the Federal Trade Commission

KATHERINE RACE BRIN
Counsel for the Federal Trade Commission

APPROVED:

MARK EICHORN
Assistant Director
Division of Privacy and Identity Protection

MANEESHA MITHAL
Associate Director
Division of Privacy and Identity Protection

DAVID C. VLADECK
Director
Bureau of Consumer Protection



[Home](#) > [News and events](#) > News > Google's new privacy policy : incomplete information and uncontrolled combination of data across services

News

Google's new privacy policy : incomplete information and uncontrolled combination of data across services

16 October 2012



After several months of investigation led by the CNIL into Google's new Privacy Policy that came into force on March 1, the EU Data Protection authorities publish their common findings. They recommend clearer information of the users and ask Google to offer the persons improved control over the combination of data across its numerous

services. Finally, they wish that Google modifies the tools it uses to avoid an excessive collection of data.

On January 24, Google announced that it would be updating its privacy policy and terms of service for almost all of its services on March 1, 2012.

Given the numerous questions raised by these changes, the Article 29 Working Party mandated the CNIL to lead the investigation into Google's new privacy policy. Two successive questionnaires were sent to Google. The company replied on April 20 and June 21, but several answers were incomplete or approximate. In particular, Google did not provide satisfactory answers on key issues such as the description of its personal data processing operations or the precise list of the 60+ product-specific privacy policies that have been merged in the new policy.

The analysis of Google's answers and the examination of numerous documents and technical mechanisms by the CNIL's experts have led EU Data protection authorities to draw their conclusions and make recommendations to Google.

Firstly, it is not possible to ascertain from the analysis that Google respects the key data protection principles of purpose limitation, data quality, data minimization, proportionality and right to object. Indeed, the Privacy policy suggests the absence of any limit concerning the scope of the collection and the potential uses of the personal data. The EU Data protection authorities challenge Google to commit publicly to these principles.

Google provides insufficient information to its users on its personal data processing operations:

Under the current Policy, a Google service's user is unable to determine which categories of personal data are processed for this service, and the exact purposes for which these data are processed.

E.g.: the Privacy Policy makes no difference in terms of processing between the innocuous content of search query and the credit card number or the telephone communications of the user ; all these data can be used equally for all the purposes in the Policy.

Moreover, passive users (i.e. those that interact with some of Google's services like advertising or '+1' buttons on third-party websites) have no information at all.

EU Data protection authorities remind Google and internet companies in general that shorter privacy notices do not justify a reduction of information delivered to the data subjects.

- EU Data protection authorities ask Google to provide clearer and

don't make it shorter!

Voir aussi

CNIL sends an additional questionnaire on Google's new privacy policy due to insufficient answers

GOOGLE's new privacy policy: CNIL sends a detailed questionnaire to Google

Google's new privacy policy raises deep concerns about data protection and the respect of the European law

Pour approfondir

Letter addressed to Google by the Article...

Annex : G29's Recommendations for Google...

more comprehensive information about the collected data and purposes of each of its personal data processing operations. For instance, EU Data protection authorities recommend the implementation of a presentation with three levels of detail to ensure that information complies with the requirements laid down in the Directive and does not degrade the users' experience. The ergonomics of the Policy could also be improved with interactive presentations.

- Google does not provide user control over the combination of data across its numerous services

Combination of data across services has been generalized with the new Privacy Policy: in practice, any online activity related to Google (use of its services, of its system Android or consultation of third-party websites using Google's services) can be gathered and combined.

The European DPAs note that this combination pursues different purposes such as the provision of a service requested by the user, product development, security, advertising, the creation of the Google account or academic research. The investigation also showed that the combination of data is extremely broad in terms of scope and age of the data.

E.g.: the mere consultation of a website including a '+1' button is recorded and kept during at least 18 months and can be associated with the uses of Google's services; data collected with the DoubleClick cookie are associated to a identifying number valid during 2-years and renewable.

European Data Protection legislation provides a precise framework for personal data processing operations. Google must have a legal basis to perform the combination of data of each of these purposes and data collection must also remain proportionate to the purposes pursued. However, for some of these purposes including advertising, the processing does not rely on consent, on Google's legitimate interests, nor on the performance of a contract.

Google should therefore modify its practices when combining data across services for these purposes, including:

- reinforce users' consent to the combination of data for the purposes of service improvements, development of new services, advertising and analytics. This could be realized by giving users the opportunity to choose when their data are combined, for instance with dedicated buttons in the services' (cf. button "Search Plus Your World"),
- offer an improved control over the combination of data by simplifying and centralizing the right to object (opt-out) and by allowing users to choose for which service their data are combined
- adapt the tools used by Google for the combination of data so that it remains limited to the authorized purposes, e.g. by differentiating the tools used for security and those used for advertising.

Google does not provide retention periods

Google refused to provide retention periods for the personal data it processes.

The recommendations of the EU Data protection authorities have been sent to Google to allow the company to upgrade its Privacy Policy practices. This letter is individually signed by 27 European Data protection authorities for the first time and it is a significant step forward in the mobilization of European authorities.

Several recommendations are also supported by members of APPA (Asia Pacific Privacy Authorities) and Canada's federal Privacy Commissioner has had similar concerns about various Google activities.

The CNIL, all the authorities among the Working Party and data protection

authorities from other regions of the world expect Google to take effective and public measures to comply quickly and commit itself to the implementation of these recommendations.

Retour

ARTICLE 29 Data Protection Working Party



Read 10/25 in class

Brussels, 16.10.2012

Dear Mr. Page,

On March 1, 2012 Google changed the privacy policy and terms of service that apply to most of its services. This new policy merges many product-specific privacy policies and generalizes combination of data across services.

We recognize that Google launched an extensive advertising campaign to inform its users about the new Privacy Policy, using various information tools (emails, pop-ups, etc.). However, the changes in the new Privacy Policy have been decided without substantial discussions with data protection regulators and have raised numerous questions about Google's processing operations.

The EU Data Protection Authorities, united within the Article 29 Working Party, launched an in-depth investigation to assess the compliance of Google's new Privacy Policy with the European Data Protection legislation, notably the Data Protection Directive 95/46/EC and the ePrivacy Directive 2002/58/EC. The Working Party asked the French Data Protection Authority (CNIL) to take the lead in this analysis. Google collaborated with the Working Party's investigation by answering two questionnaires sent by the CNIL on March 19 and May 22. Other data protection and privacy authorities around the world, like the Asia Pacific Privacy Authorities, also conducted inquiries.

Google explained that many of its privacy-related practices do not differ from other U.S. internet companies. We examine the practices of other companies operating in this sector, if needed be publicly.

As a leader in the online world, we expect Google to proactively engage on privacy matters in close relationship with the competent authorities of the countries where your company offers its services. The wide variety of processing operations implemented by Google requires a strong and enduring commitment to ensure that Google's development is not made at the expenses of your users' privacy. Therefore, we are happy that Google accepted to clarify some issues, although grey areas still remain after analyzing your answers to the two questionnaires.

In particular, Google's answers have not demonstrated that your company endorses the key data protection principles of purpose limitation, data quality, data minimization, proportionality and right to object. Indeed, the Privacy policy suggests the absence of any limit concerning the scope of the collection and the potential uses of the personal data. **We challenge you to commit publicly to these principles.**

Additionally, the investigation unveiled several legal issues with the new privacy policy and the combination of data.

Firstly, the investigation showed that Google provides insufficient information to its users (including passive users), especially on the purposes and the categories of data

What Google trying to avoid in US!

being processed. As a result, a Google user is unable to determine which categories of data are processed in the service he uses, and for which purpose these data are processed. Internet companies should not develop privacy notices that are too complex, law-oriented or excessively long. However, the search for simplicity should not lead internet companies to avoid the respect of their duties. We require from all large and global companies that they detail and differentiate their processing operations.

Secondly, **the investigation confirmed our concerns about the combination of data across services.** The new Privacy Policy allows Google to combine almost any data from any services for any purposes. Combination of data, like any other processing of personal data, requires an appropriate legal ground and should not be incompatible with the purpose for which these data were collected. For some of the purposes related to the combination of data and which are further elaborated in the appendix, Google does not collect the unambiguous consent of the user, the protection of the individual's fundamental rights and freedoms overrides Google's legitimate interests to collect such a large database, and no contract justifies this large combination of data. Google empowers itself to collect vast amounts of personal data about internet users, but Google has not demonstrated that this collection was proportionate to the purposes for which they are processed. Moreover, Google did not set any limits to the combination of data nor provide clear and comprehensive tools allowing its users to control it. Combining personal data on such a large scale creates high risks to the privacy of users. Therefore, Google should modify its practices when combining data across services for these purposes.

Other purposes are legitimate or based on consent, such as the provision of a service where the user requests the combination of data across services (e.g. access to the contacts in Calendar), security or academic research, even if improvements should be made with regard to the information provided.

Finally, Google failed to provide retention periods for the personal data it processes.

As data protection regulators, we expect that Google takes the necessary steps to improve information and clarify the combination of data, and more generally ensure compliance with data protection laws and principles. To that end, we list below our practical recommendations. You will also find a summary of the findings of the investigation and detailed recommendations in the appendix.

Regarding **information**, Google should disclose and detail how it processes personal data in each service and differentiate the purposes for each service and each category of data. In practice, Google could:

- Define an architecture of layered privacy notices with three levels: (1st level) in-product privacy notices and interstitial notices, (2nd level) the current privacy policy in an updated version, (3rd level) product-specific information;
- Develop interactive presentations that allow users to navigate easily through the content of the policies;
- Provide additional and precise information about data that have a significant impact on users (location, credit card data, unique device identifiers, telephony, biometrics)
- Adapt information to mobile users;
- Ensure that passive users are appropriately informed.

The implementation of these recommendations would ensure comprehensive, non-invasive and clear information for the data subjects.

Regarding **combination of data**, Google should take action to clarify the purposes and means of the combination of data. In that perspective, Google should detail more clearly how data is combined across its services and develop new tools to give users more control over their personal data. This could be done by implementing the following controls (detailed in appendix):

- Simplify opt-out mechanisms for authenticated and non-authenticated users, and make them available in one place;
- Differentiate the purposes of the combination of data with appropriate tools;
- Collect explicit consent for the combination of data for certain purposes;
- Offer the possibility for authenticated users to control in which service they are logged in;
- Limit the combination of data for passive users;
- Implement Article 5(3) of the European ePrivacy Directive;
- Extend to all countries the process designed for Google Analytics in Germany.

We recognize Google's key role in the online world. Our recommendations do not seek to limit the company's ability to innovate and improve its products, but rather to strengthen users' trust and control, and to ensure compliance with data protection legislations and principles.

Finally, we encourage you to engage with data protection authorities when developing services with significant implications for privacy.

We would like you to send a response to the CNIL indicating how and within what timeframe Google will update its privacy policy and practices to implement our recommendations.

Yours sincerely,

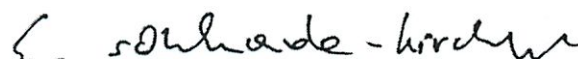
Isabelle FALQUE-PIERROTIN (FR)



Jacob KOHNSTAMM (Chairman Article 29 Working Party + NL)



Eva SOUHRADA-KIRCHMAYER (AT)



Willem DEBEUCKELAERE (BE)

Mariya Mateva
Krassimir DIMITROV (BG)

Igor NEMEC (CZ)

Peter SCHAAR (DE)

Janni CHRISTOFFERSEN (DK)

Stina Lührand
Viljar PEEP (EE)
on behalf of

Petros Christoforos
Petros CHRISTOFOROS (EL)

José Luis RODRÍGUEZ ÁLVAREZ (ES)

Reijo AARNIO (FI)

Billy HAWKES (IE)

Antonello SORO (IT)

Attila PÉTERFALVI (HU)
Eudre Győző SZABÓ

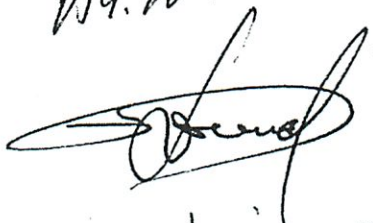


Yiannos DANIELIDES (CY)

Algirdas KUNČINAS (LT)



Gérard LOMMEL (LU)



Joseph EBEJER (MT)



Wojciech Rafał WIEWIÓROWSKI (PL)

On behalf of Mr. Henryk Wiewiórowski
Kub G

Filipa CALVÃO (PT)



Göran GRÄSLUND (SE)



Natasa PIRC MUSAR (SI)



Eleonóra KROČIANOVÁ (SK)



Christopher GRAHAM (UK)



DUBRAVKO BILIĆ (HR)



Philipp Mittelboeck (Liechtenstein)



Read 10/25 Jaldass

APPENDIX

GOOGLE PRIVACY POLICY: MAIN FINDINGS AND RECOMMENDATIONS

OUTLINE

I. Main findings.....	2
1) Legal Framework.....	2
2) Information	2
3) Combination of data across services	3
4) Retention period	5
II. Recommendations	5
1) Information	5
i. Particular case of mobile users	6
ii. Particular case of passive users	7
2) Combination of data	7
i. For purposes that have a legal basis for the combination of data (cases #1, #3, #5, #8)	7
ii. For purposes that do not have a legal basis for the combination of data (cases #2, #4, #6, #7)	7
iii. Practical recommendations	7
iv. Particular case of Google Apps (Free edition) users	8
3) Retention period	8
III. Others	8
1) Name policy	8
2) Facial recognition	8
3) International transfers and safe harbor	9

I. MAIN FINDINGS

1) LEGAL FRAMEWORK

Google's services¹ are available to natural persons in the European Union and the criteria of the European Directive to define applicable law are met. The European Data Protection law therefore applies to Google's personal data processing operations.

Google implements several personal data processing operations in the course of the provision of its services: a specific processing operation can be associated with each service and Google implements other processing operations for crosscutting purposes such as security, research, etc.

The Working Party identified three types of data subjects that use Google's services:

- Authenticated users (Gmail, Google Play, Docs, Google+, etc.)
- Non-authenticated users (Search, Maps, Youtube, etc.)
- Passive users (DoubleClick, Analytics, '+1' buttons)² *How is that diff*

2) INFORMATION

Google's Privacy Policy fails to respect the obligation of information, laid down in section IV of the Data protection directive.

First, Google gives incomplete or approximate information about the purposes and the categories of data collected. The Privacy Policy is a mix of particularly wide statements and of examples that mitigate these statements and mislead users on the exact extent of Google's actual practices. Additional information is available in in-product privacy notices, the Help Center or blogs but the information available in these documents is inconsistent between the different sources or spoken languages, can be changed at any moment and is sometimes difficult to understand. The main Privacy Policy is the only traceable document (i.e. for which previous versions are still available). The Working Party notes in particular that the 60+ previous privacy policies that have been merged in the main Privacy Policy are not available anymore and that Google failed to provide the list of these 60+ privacy policies.

Regarding information on purposes, the purposes in the Privacy Policy are not detailed enough and do not respect the principle of purpose limitation. Either the purposes in the Policy are the actual purposes of Google's processings, in which case Google does not comply with Article 6(b)

¹ Google's services are provided in 22 of the 23 official languages of the European Union (all except Maltese – regional and other national official languages may also be available) and Google's services are available in 25 of the 27 main top-level domains of the Member States (all except .mt and .cy – google.eu is not available either). Besides the availability of Google's online services, devices running Google's software (mainly Android phones) are commercialized in most if not all Member States. Google also owns national companies established in several European countries (e.g. in the UK, Ireland and France), which are to some extent involved in commercial purposes, research and development, and public relations. Google's headquarters in Europe are located in Dublin, Ireland. Google uses servers located in the European Union to provide its services, including two major datacenters located in Belgium and Finland. Google also uses cookies and other means, stored on users' devices, to provide its services.

² Passive users, as defined in the questionnaire sent on March 16 are users who does not directly request a Google service but from whom data is still collected, typically through third party ad platforms, analytics or +1 buttons.

of the Directive (because purposes are not “specified and explicit”), or personal data are processed for more specific purposes that Google did not describe in the Privacy Policy and in its answers to the questionnaires: in this case, Google failed to comply with the obligation of information defined in Articles 10 and 11 of the Data Protection Directive.

Regarding information on the categories of data that are processed by the services, the categories described in the privacy policy are too broad and do not provide appropriate information to the data subject when he uses a particular service.

The actual use of data by Google in each service may not be excessive but in this case, information is insufficient with respect to the requirements laid down in Articles 10 and 11 of the Directive. Google also failed to provide elements that would guarantee the respect of the principle of data minimization. In particular, Google has not indicated what data is combined between which services.

Concerning passive users, users are generally not informed that Google is processing personal data, such as IP addresses and cookies. Information depends on the website’s policy and may often not detail Google’s processing.

3) COMBINATION OF DATA ACROSS SERVICES

Google uses many tools to combine data:

- The Google Account associated with each authenticated user
- The PREF cookie associated with each interaction with a website of the google.com domain (including ‘+1’ buttons on third-party websites)
- The DoubleClick cookie associated with interactions on third-party websites that display DoubleClick advertisements
- The Google Analytics cookie used by third-party websites
- Mobile identifiers used to replace cookies on some mobile applications

The combination of data implemented by Google is very broad as it will include all the activity of data subjects on Google’s sites³ and activity on third-party websites (‘+1’ buttons, DoubleClick). Google also stores data during long periods of time: 18 months of browsing history for the PREF cookie, 2 years for the advertising cookie. Furthermore, the risks associated with the combination of data across services are high for the data subjects: data breach, rogue personnel, legal requests, etc.

The Working Party identified 8 different purposes for the combination of data across Google’s services:

- The provision of **services where the user requests the combination of data (case #1)** (e.g. Contacts & Gmail)
- The provision of services requested by the user but where the combination of data applies **without the user’s direct knowledge (case #2)** (e.g. search results personalization)
- **Security purposes (case #3)**

³ Google has a European market share of around 90% for search and around 50% for smartphone OS

- **Product development and marketing innovation purposes (case #4)**
- **The provision of the Google Account (case #5)**
- **Advertising purposes (case #6)**
- **Analytics purposes (case #7)**
- **Academic research purposes (case #8)**

However, the tools used by Google such as the Google Account or the PREF cookie have use policies that are independent of the purposes, e.g. anonymisation of server logs after 18 months. Google does not differentiate the different purposes for the combination of data and does not clearly endorse the principle of purpose limitation.

Additionally, the Working Party examined the lawfulness of the combination of data in regards of the legal grounds set out in Article 7 of the Directive, namely "consent", "performance of a contract" and "legitimate interests".

For four of the eight purposes above, the Working Party has established the absence of a legal ground **for the combination of data across services**⁴. This is the case for the provision of services where the combination of data applies without the user's direct knowledge (case #2), marketing innovation and product development (#4), advertising purposes (#6) and analytics purposes (#7).

For these purposes, there is **no valid consent** from the user, in particular because the user is not aware of the exact extent of the combination of data. **Google's interests** to implement the extensive combination of data detailed above **are overridden by the interests for fundamental rights and freedoms of the data subject** and therefore, the legal ground of the ~~legitimate interests~~ may not apply, unless Google clearly limits the scope and duration of the combination of data and provides simple and effective rights to the data subjects. Finally, Google did not provide significant examples of combination of data realized for the performance of a contract that would justify such a large collection and combination of data.

Google may not claim to use any data from any service for these purposes without a valid legal basis. In order to remedy to this situation, **Google should seek consent from the data subjects for the combination of data for these purposes and provide additional controls to users regarding these combinations.**

The new Privacy Policy also applies to end-users of the Google Apps (Free) offer. In this case, consent may not be valid because the data subject is likely to be an employee of the customer of Google that decides to use this offer.

More generally and for all purposes, **combination of data must respect the principles of proportionality, purpose limitation, data minimization and right to object.** Google does not publicly endorse these principles and failed to provide clear and definite answers on these matters: there is no guarantee that only the data necessary to the purpose is combined, information is insufficient (cf. section "Information") and the current opt-out mechanisms are too complex and ineffective. For instance, a mobile authenticated Google+ user who does not want personalized ads must perform six different opt-outs. Moreover, some of the mechanisms do not prevent the collection of data, but only the display of personalized content. Finally, there

⁴The investigation does not assess the legal ground of Google's processing operations besides the combination of data.

are no opt-outs for the purposes of research or marketing innovation and product development except by not using the service.

For **passive users**, Google does not respect Article 5(3) of the ePrivacy Directive regarding cookies triggered by DoubleClick, '+1' buttons or Google Analytics services on third-party websites. Informed consent is necessary before these cookies are used for the purpose of data combination across services.

Regarding **Google Analytics** and the combination of data for analytics purposes, specific safeguards have been implemented for German users: data combination across services is excluded, a specific contract is signed between Google and the website, and customers can automatically anonymise the IP address shared with Google. Such conditions can provide adequate protection of personal data and should be extended to all European Member States.

4) RETENTION PERIOD

Despite the numerous and detailed questions of the Working Party, Google has been unable to provide a maximum or typical retention period for the personal data it processes. This absence of response questions the effectiveness of the opt-out mechanisms and deletion actions requested by the users.

The Working Party encourages Google to endorse the principle of retention period strictly limited according to the purposes.

II. RECOMMENDATIONS

Considering the conclusions of the investigation, Google should implement the following recommendations in order to comply with the Data protection legislation.

1) INFORMATION

To remedy the insufficient information about Google's processings, **Google must complete information about its processing operations by detailing for each processing the exact purposes and collected data (including data from other services)**.

Information must describe the purposes and the categories of data processed in a clear and accurate manner. The processing operation itself must be conducted with due respect to the rules of proportionality and data minimisation, which must be reflected in the information that is delivered.

Moreover, notices about each processing must not be modified unless the user has given his consent, having been provided with clear and comprehensive information inter alia about the changes to be implemented; furthermore, notices should be traceable.

Practically, the Working Party recommends to define an architecture of privacy notices that would offer a simple and comprehensive information about the processing operations. Users

should have a clear visibility on this architecture and be able to navigate in ways that meet their expectations.

The architecture could adopt the following three levels:

Architecture is good names

First, **in-product privacy notices and interstitial notices** could be developed to increase user's awareness of the processing when they use the services and especially when they launch a new service for the first time. Tools such as the toggle button for "Search Plus Your World" or the "butter-buttons" used to inform about the change of Privacy Policy are also good examples of straightforward and timely information. Google should develop internal processes to systematically verify the level of basic user information regarding personal data protection for each of its existing and future services.

Second, the **current privacy policy** should be presented as a general guideline about Google's processing operations and references should be made to more detailed information about the different processings ("product-specific privacy notices"). Moreover, the Working Party recommends separating clearly the statements of the policy from illustrative examples, as these examples tend to mislead the users about the exact scope of the statements. Examples should also ideally cover different use cases. The Privacy Policy should include all types of categories of data, including biometric data, as face recognition is not mentioned in the current policy.

Third, **product-specific privacy notices** should be made available. Such notices should detail for each processing and service: the data that is processed, the purposes of the processing, the recipients and how users can access their data. General purposes such as research and security could be presented separately with detailed guarantees about these purposes. Previous versions of the privacy policy and of the product-specific privacy notices should remain available to users.

More generally, Google should develop interactive presentations that allow users to explore the content of the privacy notices without having to read long and linear documents.

Finally, Google should provide additional and precise information about the following data that may have significant impact on the privacy of users:

- Location
- Credit card data
- Unique device identifiers
- Telephony

bl
↳ w/ European production company

Users must have simple and clear explanations on when, why and how such data are collected and how they can oppose to the collection, the storage or the combination of these data.

i. PARTICULAR CASE OF MOBILE USERS

Mobile users face the additional challenge to use Google's services on small screens, with limited interactions. Many of the features requested above may not appear or may not be delivered on mobile screens, especially in-product privacy notices or interactive presentations.

Google must provide adapted information for these users, possibly with specific tools that may include dedicated applications or privacy controls on Android.

ii. PARTICULAR CASE OF PASSIVE USERS

Regarding passive users, information is mainly delivered by third-party websites on which Google's services are implemented. Google must therefore make sure users are correctly informed about the processing operations that concern them.

2) COMBINATION OF DATA

Regarding the combination of data, Google lacks a legal basis for certain purposes. Furthermore, information about the combination of data is particularly weak and the recommendations of the previous section apply: Google must first reinforce information to clarify the data that is combined across services and the purposes for which data is combined.

i. FOR PURPOSES THAT HAVE A LEGAL BASIS FOR THE COMBINATION OF DATA (CASES #1, #3, #5, #8)

When using data from other services, Google must adopt a Privacy by Design approach: limited sets of personal data should be used, and anonymisation should be implemented, when possible (principle of data minimisation).

Simple opt-outs must be made available for the purposes where the right to object applies, i.e. provision of services requested by the user (case #1), research (#8) and Google Profile (#5). In general, opt-out for security purposes requires a cautious approach to avoid abuses.

Retention periods must be appropriate in regards to the purpose.

ii. FOR PURPOSES THAT DO NOT HAVE A LEGAL BASIS FOR THE COMBINATION OF DATA (CASES #2, #4, #6, #7)

Google must seek unambiguous consent from the data subjects for these purposes and limit clearly the scope of the combination of data in proportion with the purposes pursued.

In this context, the inclusion of a new service into the combination of data or a new purpose requires explicit consent (e.g. Google Now), that can be easily collected the first time a user wishes to use the new service.

hard since most just want it for work

The Working Party also advises Google to develop new tools to allow users to control which services may combine data. These controls can include:

- Specific settings in the Google Dashboard for authenticated users
- Explicit consent and improved control over cookies (and the data collected) for non-authenticated and passive users

iii. PRACTICAL RECOMMENDATIONS

The following practical recommendations could therefore be implemented by Google to ensure legal compliance of the combination of data:

1. Google should simplify the opt-out mechanisms and foresee new tools to implement the right to object to the combination of data for some of the purposes detailed above. In this regard, user should have a clear understanding of the purposes for which data is combined.

2. Google should **differentiate the purposes of the combination of data** with appropriate tools: the use of the PREF cookie ID for several purposes should be abandoned and cookies (or other tools) could be created for each purpose (security, advertising, service improvements) with retention policies and access rights related to the purpose.
3. Google should **collect explicit consent for the combination of data** for the purposes of service improvements without the user's direct knowledge, product development and marketing innovation, advertising and analytics.
4. Google should make the **opt-out mechanisms available in one place** for authenticated and non-authenticated users.
5. Google should offer the option for authenticated users to **control in which service they are logged in** when these services are available without authentication (e.g. Search, Maps or Youtube), typically with a setting on their account.
6. Google should limit the collection and combination of data from passive users, except for security purposes.
7. Google must **enforce Article 5(3)** of the ePrivacy Directive for passive users, with regards to the guidance provided in the WP29 Opinion on Cookie consent exemption. *So silly*
8. For analytics purposes, Google should also **extend to all European users the process designed in Germany** (enhanced information of the data subjects by the website, limited use of the data to the purpose of analytics and IP anonymisation).

iv. PARTICULAR CASE OF GOOGLE APPS (FREE EDITION) USERS

For Google Apps end-users, the use of a Google Account is decided by the Google Apps customer (typically the company that employs the end-users): consent may therefore not be valid. Google should apply limitations to the combination of data across services and this combination should be restricted to the services included in the Google Apps offer.

3) RETENTION PERIOD

Google should define more clearly the retention period of personal data, especially for the following actions: deletion of a particular content, unsubscription of a specific service, deletion of the account.

III. OTHERS

1) NAME POLICY

Google must inform new users more clearly that they can sign-up to a Google account without providing their real name.

2) FACIAL RECOGNITION

Google must complete the Privacy Policy by mentioning that biometric data may be processed and clarify the conditions of collection and storage of the face template.

3) INTERNATIONAL TRANSFERS AND SAFE HARBOR

Google's compliance with the European rules applicable to international transfers and to the U.S.-E.U. Safe Harbor Agreement has not been investigated in this analysis.

Innovation Insights

Community blog about cloud computing

› Expand/Collapse

› **Contributor Content**

› Cloud/Storage

› Data Tools

› IBM Sponsored Content

› Software-Defined Networking

› Supercomputers

› The Personal Cloud

› Cloud

› Featured

› Blog

Like

Google: Let Us Opt Out of Your Data Mining Machine

› By Doug Miller

› 10.17.12

› 12:05 PM



Would you opt out of Google's online data collection if you could? Should we be able to? Have your say in the Insights forum below. *Image: zampano1212/Flickr*

The French data protection agency (aka, the CNIL), acting on behalf of a large group of European data protection agencies, today announced that it was taking action to push Google to make a number of changes to its privacy policy that came into effect earlier this year. One of the big issues for the CNIL is the lack of control for the user over the amount of data that is collected when you use a Google cloud service or how that data can be used. There is

no opt-out for users if they don't want their browsing habits and internet content mined for the purpose of enhancing Google's search or displaying more relevant Google ads.

Google's answer to this is "competition is one click away." If you don't like how Google treats your private data then you can use someone else's product.

Yet this answer does not ring true for users who are forced to use Google's services because their employer or school has adopted Google Apps for Business, Education and Government.

In this case, your employer or school has signed up for Google Apps but you, as the user, are the one who has to live with the data mining that goes on every time you use the service.

Somehow this does not seem right. All Google Apps organizations that pay for these services and their users should have the ability to not pass any data back to Google beyond what is needed to run the service they have signed up for. *Getting cheaper price*

Google will tell you that special privacy agreements apply to enterprises, schools and governments but there is increasing evidence that this is simply not true. A visit to Google's own web pages promoting these services always takes you back to the same privacy agreement that the Europeans have an issue with. The same privacy policy that is used in Google's free consumer-oriented services. The same agreement that gives Google the right use pretty much everything that happens in your internet session and mine any data that is input while you are using any Google service. This includes your Gmail, your Google searches, what YouTube videos you watch, your Google+ posts, which numbers you call on your Android phone, and where you are located when you use a Google service. How does Google use this information (another question the European's have asked)? The answer is pretty clear if you read the Google privacy policy. It uses this information to enhance search results, display more relevant ads, to improve existing services and to develop new services.

So, you may ask, what has this got to do with having an email account for a business or school, or creating documents for a government job? Well — nothing actually. None of this is required for providing these services. You could even go so far as to say that this is none of Google's business. Yet in reality, this is exactly Google's business. This data collection is purely to benefit Google — the company that has stated it wants to organize the world's information (including all of your information) and the company that makes about \$40 billion a year from advertising based on leveraging all that data that it has "organized."

The Europeans are onto something here and we in North America need to pay attention. As individuals, students and workers, we cannot afford to let this become the norm for cloud services. Google, give us our digital lives back and let us opt out from your data mining machine.

Discuss this post:

Should We Be Able to Opt-Out of Google's Data Mining?

The French data protection agency (aka the CNIL), acting on behalf of a large group of European data protection agencies, today announced that it was taking action to push Google to make a number of changes to its privacy policy that came into effect earlier this year, writes Insights contributor Doug Miller.

Cutting to the chase here:

So, you may ask, what has this got to do with having an email account for a business or school, or creating documents for a government job? Well — nothing actually. None of this is required for providing these services. You could even go so far as to say that this is none of Google's business. Yet in reality, this is exactly Google's business. This data collection is purely to benefit Google - the company that has stated it wants to organize the world's information (including all of your information)

Read 11/3 + 11/16

CONSUMER DATA PRIVACY
IN A NETWORKED WORLD:
A FRAMEWORK FOR PROTECTING
PRIVACY AND PROMOTING INNOVATION
IN THE GLOBAL DIGITAL ECONOMY

FEBRUARY 2012





THE WHITE HOUSE
WASHINGTON

February 23, 2012

Americans have always cherished our privacy. From the birth of our republic, we assured ourselves protection against unlawful intrusion into our homes and our personal papers. At the same time, we set up a postal system to enable citizens all over the new nation to engage in commerce and political discourse. Soon after, Congress made it a crime to invade the privacy of the mails. And later we extended privacy protections to new modes of communications such as the telephone, the computer, and eventually email.

Justice Brandeis taught us that privacy is the "right to be let alone," but we also know that privacy is about much more than just solitude or secrecy. Citizens who feel protected from misuse of their personal information feel free to engage in commerce, to participate in the political process, or to seek needed health care. This is why we have laws that protect financial privacy and health privacy, and that protect consumers against unfair and deceptive uses of their information. This is why the Supreme Court has protected anonymous political speech, the same right exercised by the pamphleteers of the early Republic and today's bloggers.

Never has privacy been more important than today, in the age of the Internet, the World Wide Web and smart phones. In just the last decade, the Internet has enabled a renewal of direct political engagement by citizens around the globe and an explosion of commerce and innovation creating jobs of the future. Much of this innovation is enabled by novel uses of personal information. So, it is incumbent on us to do what we have done throughout history: apply our timeless privacy values to the new technologies and circumstances of our times.

I am pleased to present this new Consumer Privacy Bill of Rights as a blueprint for privacy in the information age. These rights give consumers clear guidance on what they should expect from those who handle their personal information, and set expectations for companies that use personal data. I call on these companies to begin immediately working with privacy advocates, consumer protection enforcement agencies, and others to implement these principles in enforceable codes of conduct. My Administration will work to advance these principles and work with Congress to put them into law. With this Consumer Privacy Bill of Rights, we offer to the world a dynamic model of how to offer strong privacy protection and enable ongoing innovation in new information technologies.

One thing should be clear, even though we live in a world in which we share personal information more freely than in the past, we must reject the conclusion that privacy is an outmoded value. It has been at the heart of our democracy from its inception, and we need it now more than ever.

What force of law
does this have?



Foreword

Trust is essential to maintaining the social and economic benefits that networked technologies bring to the United States and the rest of the world. With the confidence that companies will handle information about them fairly and responsibly, consumers have turned to the Internet to express their creativity, join political movements, form and maintain friendships, and engage in commerce. The Internet's global connectivity means that a single innovator's idea can grow rapidly into a product or service that becomes a daily necessity for hundreds of millions of consumers. American companies lead the way in providing these technologies, and the United States benefits through job creation and economic growth as a result. Our continuing leadership in this area depends on American companies' ability to earn and maintain the trust of consumers in a global marketplace.

Privacy protections are critical to maintaining consumer trust in networked technologies. When consumers provide information about themselves—whether it is in the context of an online social network that is open to public view or a transaction involving sensitive personal data—they reasonably expect companies to use this information in ways that are consistent with the surrounding context. Many companies live up to these expectations, but some do not. Neither consumers nor companies have a clear set of ground rules to apply in the commercial arena. As a result, it is difficult today for consumers to assess whether a company's privacy practices warrant their trust.

The consumer data privacy framework in the United States is, in fact, strong. This framework rests on fundamental privacy values, flexible and adaptable common law protections and consumer protection statutes, Federal Trade Commission (FTC) enforcement, and policy development that involves a broad array of stakeholders. This framework has encouraged not only social and economic innovations based on the Internet but also vibrant discussions of how to protect privacy in a networked society involving civil society, industry, academia, and the government. The current framework, however, lacks two elements: a clear statement of basic privacy principles that apply to the commercial world, and a sustained commitment of all stakeholders to address consumer data privacy issues as they arise from advances in technologies and business models.

To address these issues, the Administration offers *Consumer Data Privacy in a Networked World*. At the center of this framework is a Consumer Privacy Bill of Rights, which embraces privacy principles recognized throughout the world and adapts them to the dynamic environment of the commercial Internet. The Administration has called for Congress to pass legislation that applies the Consumer Privacy Bill of Rights to commercial sectors that are not subject to existing Federal data privacy laws. The Federal Government will play a role in convening discussions among stakeholders—companies, privacy and consumer advocates, international partners, State Attorneys General, Federal criminal and civil law enforcement representatives, and academics—who will then develop codes of conduct that implement the Consumer Privacy Bill of Rights. Such practices, when publicly and affirmatively adopted by companies subject to Federal Trade Commission jurisdiction, will be legally enforceable by the FTC. The United States will engage with our international partners to create greater interoperability among our

CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING
PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY

respective privacy frameworks. This will provide more consistent protections for consumers and lower compliance burdens for companies.

Of course, this framework is just a beginning. Starting now, the Administration will work with and encourage stakeholders, including the private sector, to implement the Consumer Privacy Bill of Rights. The Administration will also work with Congress to write these flexible, general principles into law. The Administration is ready to do its part as a convener to achieve privacy protections that preserve consumer trust and promote innovation.



Table of Contents

Executive Summary	1
I. Introduction: Building on the Strength of the U.S. Consumer Data Privacy Framework	5
II. Defining a Consumer Privacy Bill of Rights	9
III. Implementing the Consumer Privacy Bill of Rights: Multistakeholder Processes to Develop Enforceable Codes of Conduct	23
A. Building on the Successes of Internet Policymaking	25
B. Defining the Multistakeholder Process for Consumer Data Privacy	26
III. Building on the FTC's Enforcement Expertise.	29
A. Protecting Consumers Through Strong Enforcement.	29
B. Providing Incentives to Develop Enforceable Codes of Conduct	29
III. Promoting International Interoperability	31
A. Mutual Recognition.	31
B. An International Role for Multistakeholder Processes and Codes of Conduct	33
C. Enforcement Cooperation	33
IV. Enacting Consumer Data Privacy Legislation.	35
A. Codify the Consumer Privacy Bill of Rights	35
B. Grant the FTC Direct Enforcement Authority	36
C. Provide Legal Certainty Through an Enforcement Safe Harbor	37
D. Balance Federal and State Roles in Consumer Data Privacy Protection	37
E. Preserve Effective Protections in Existing Federal Data Privacy Laws	38
F. Set a National Standard for Security Breach Notification	39
VII. Federal Government Leadership in Improving Individual Privacy Protections	41
A. Enabling New Services	41
B. Protecting Privacy Through Effective Enforcement.	42
C. Guidance for Protecting Privacy	43
D. Integrating Privacy Into the Structure of Federal Agencies.	44

CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING
PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY

VIII. Conclusion	45
IX. Appendix A: The Consumer Privacy Bill of Rights	47
X. Appendix B: Comparison of the Consumer Privacy Bill of Rights to Other Statements of the Fair Information Practice Principles (FIPPs).	49

The Consumer Privacy Bill of Rights provides general principles that afford companies discretion in how they implement them. This flexibility will help promote innovation. Flexibility will also encourage effective privacy protections by allowing companies, informed by input from consumers and other stakeholders, to address the privacy issues that are likely to be most important to their customers and users, rather than requiring companies to adhere to a single, rigid set of requirements.

Enacting the Consumer Privacy Bill of Rights through Federal legislation would increase legal certainty for companies, strengthen consumer trust, and bolster the United States' ability to lead consumer data privacy engagements with our international partners. Even if Congress does not pass legislation, the Consumer Privacy Bill of Rights will serve as a template for privacy protections that increase consumer trust on the Internet and promote innovation.

- **Fostering Multistakeholder Processes to Develop Enforceable Codes of Conduct**

The Administration's framework outlines a multistakeholder process to produce enforceable codes of conduct that implement the Consumer Privacy Bill of Rights. The Administration will convene open, transparent forums in which stakeholders who share an interest in specific markets or business contexts will work toward consensus on appropriate, legally enforceable codes of conduct. Private sector participation will be voluntary and companies ultimately will choose whether to adopt a given code of conduct. The participation of a broad group of stakeholders, including consumer groups and privacy advocates, will help to ensure that codes of conduct lead to privacy solutions that consumers can easily use and understand. A single code of conduct for a given market or business context will provide consumers with more consistent privacy protections than is common today, when privacy practices and the information that consumers receive about them varies significantly from company to company.

- **Strengthening FTC Enforcement**

FTC enforcement is critical to ensuring that companies are accountable for adhering to their privacy commitments. Enforcement is also critical to ensuring that responsible companies are not disadvantaged by competitors who would play by different rules. As part of consumer data privacy legislation, the Administration encourages Congress to provide the FTC (and State Attorneys General) with specific authority to enforce the Consumer Privacy Bill of Rights.

- **Improving Global Interoperability**

The Administration's framework embraces the goal of increased international interoperability as a means to provide consistent, low-barrier rules for personal data in the user-driven and decentralized Internet environment. The two principles that underlie our approach to interoperability are mutual recognition and enforcement cooperation. Mutual recognition depends on effective enforcement and well-defined accountability mechanisms. Multistakeholder processes can provide scalable, flexible means of developing codes of conduct that simplify companies' compliance obligations. Enforcement cooperation helps to ensure that countries are able to protect their citizens' rights when personal data crosses national boundaries. These approaches



Executive Summary

Strong consumer data privacy protections are essential to maintaining consumers' trust in the technologies and companies that drive the digital economy. The existing framework in the United States effectively addresses some privacy issues in our increasingly networked society, but additional protections are necessary to preserve consumer trust. The framework set forth in this document will provide these protections while promoting innovation.

The Administration's framework consists of four key elements: A Consumer Privacy Bill of Rights, a multistakeholder process to specify how the principles in the Consumer Privacy Bill of Rights apply in particular business contexts, effective enforcement, and a commitment to increase interoperability with the privacy frameworks of our international partners.

- **A Consumer Privacy Bill of Rights**

This document sets forth a Consumer Privacy Bill of Rights that, in the Administration's view, provides a baseline of clear protections for consumers and greater certainty for companies. The Administration will encourage stakeholders to implement the Consumer Privacy Bill of Rights through codes of conduct and will work with Congress to enact these rights through legislation. The Consumer Privacy Bill of Rights applies comprehensive, globally recognized Fair Information Practice Principles (FIPPs) to the interactive and highly interconnected environment in which we live and work today. Specifically, it provides for:

- Individual Control: Consumers have a right to exercise control over what personal data companies collect from them and how they use it.
- Transparency: Consumers have a right to easily understandable and accessible information about privacy and security practices.
- Respect for Context: Consumers have a right to expect that companies will collect, use, and disclose personal data in ways that are consistent with the context in which consumers provide the data.
- Security: Consumers have a right to secure and responsible handling of personal data.
- Access and Accuracy: Consumers have a right to access and correct personal data in usable formats, in a manner that is appropriate to the sensitivity of the data and the risk of adverse consequences to consumers if the data is inaccurate.
- Focused Collection: Consumers have a right to reasonable limits on the personal data that companies collect and retain.
- Accountability: Consumers have a right to have personal data handled by companies with appropriate measures in place to assure they adhere to the Consumer Privacy Bill of Rights.

Not policy interoperability

EXECUTIVE SUMMARY

will guide United States efforts to clarify data protections globally while ensuring the flexibility that is critical to innovation in the commercial world.

The Administration will implement this framework without delay. In the coming months, the Department of Commerce will work with other Federal agencies to convene stakeholders, including our international partners, to develop enforceable codes of conduct that build on the Consumer Privacy Bill of Rights.



I. Introduction: Building on the Strength of the U.S. Consumer Data Privacy Framework

The Internet is integral to economic and social life in the United States and throughout the world. Networked technologies offer individuals nearly limitless ways to express themselves, form social connections, transact business, and organize politically. Networked technologies also spur innovation, enable new business models, and facilitate consumers' and companies' access to information, products, and services markets across the world.

An abundance of data, inexpensive processing power, and increasingly sophisticated analytical techniques drive innovation in our increasingly networked society. Political organizations and candidates for public office build powerful campaigns on data that individuals share about themselves and their political preferences. Data from social networks allows journalists and individuals to report and follow newsworthy events around the world as they unfold. Data plays a key role in the ability of government to stop identity thieves and protect public safety. Researchers use sets of medical data to identify public health issues and probe the causes of human diseases. Network operators use data from communications networks to identify events ranging from a severed fiber optic cable to power outages and the acts of malicious intruders. In addition, personal data fuels an advertising marketplace that brings many online services and sources of content to consumers for free.

Strengthening consumer data privacy protections in the United States is an important Administration priority.¹ Americans value privacy and expect protection from intrusions by both private and governmental actors. Strong privacy protections also are critical to sustaining the trust that nurtures Internet commerce and fuels innovation. Trust means the companies and technical systems on which we depend meet our expectations for privacy, security, and reliability.² In addition, United States leadership in consumer data privacy can help establish more flexible, innovation-enhancing privacy models among our international partners.³

lol

1. This framework is concerned solely with how private-sector entities handle personal data in commercial settings. A separate set of constitutional and statutory protections apply to the government's access to data that is in the possession of private parties. In addition, the Privacy Act of 1974, Pub. L. No. 93-579 (5 U.S.C. § 552a), and implementing guidance from the Office of Management and Budget, *available at* http://www.whitehouse.gov/omb/privacy_general, govern the Federal government's handling of personally identifiable information. Both of these areas are beyond the scope of this document.

2. Throughout this document, "company" means any organization, corporation, trust, partnership, sole proprietorship, unincorporated association, or venture established to make a profit, or nonprofit entity, that collects, uses, discloses, stores, or transfers personal data in interstate commerce, to the extent such organizations are not subject to existing Federal data privacy laws.

3. See, e.g., Remarks of Secretary of State Hillary Rodham Clinton, Release of Administration's International Strategy for Cyberspace (May 2011) ("Many of you representing the governments of other countries, as well as the private sector or foundations or civil society groups, share our commitment to ensuring that the Internet remains open, secure, free, not only for the 2 billion people who are now offline, but for the billions more who will be online in the years ahead.").

CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING
PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY

Preserving trust in the Internet economy protects and enhances substantial economic activity.⁴ Online retail sales in the United States total \$145 billion annually.⁵ New uses of personal data in location services, protected by appropriate privacy and security safeguards, could create important business opportunities.⁶ Moreover, the United States is a world leader in exporting cloud computing, location-based services, and other innovative services. To preserve these economic benefits, consumers must continue to trust networked technologies. Strengthening consumer data privacy protections will help to achieve this goal.

Preserving trust also is necessary to realize the full social and cultural benefits of networked technologies. When companies use personal data in ways that are inconsistent with the circumstances under which consumers disclosed the data, however, they may undermine trust. For example, individuals who actively share information with their friends, family, colleagues, and the general public through websites and online social networking sites may not be aware of the ways those services, third parties, and their own associates may use information about them. Unauthorized disclosure of sensitive information can violate individual rights, cause injury or discrimination based on sensitive personal attributes, lead to actions and decisions taken in response to misleading or inaccurate information, and contribute to costly and potentially life-disrupting identity theft.⁷ Protecting Americans' privacy by preventing identity theft and prosecuting identity thieves is an important focus for the Administration.

The existing consumer data privacy framework in the United States is flexible and effectively addresses some consumer data privacy challenges in the digital age. This framework consists of industry best practices, FTC enforcement, and a network of chief privacy officers and other privacy professionals who develop privacy practices that adapt to changes in technology and business models and create a growing culture of privacy awareness within companies. Much of the personal data used on the Internet, however, is not subject to comprehensive Federal statutory protection, because most Federal data privacy statutes apply only to specific sectors, such as healthcare, education, communications, and financial services or, in the case of online data collection, to children. The Administration believes that filling gaps in the existing framework will promote more consistent responses to privacy concerns across the wide range of environments in which individuals have access to networked technologies and in which a broad array of companies collect and use personal data. The Administration, however, does not recommend modifying the existing Federal statutes that apply to specific sectors unless they set inconsistent standards for related technologies. Instead, the Administration supports legislation that would supplement the existing framework and extend baseline protections to the sectors that existing Federal statutes do not cover. hmm

4. President Barack Obama, *International Strategy for Cyberspace*, at 8, May 2011, http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

5. U.S. Census Bureau, *E-Stats*, May 26, 2011, <http://www.census.gov/econ/estats/2009/2009reportfinal.pdf>, at 1.

6. McKinsey Global Institute, *Big Data: The Next Frontier for Innovation, Competition, and Productivity*, at 94-95, May 2011, http://www.mckinsey.com/mgi/publications/big_data/pdfs/MGI_big_data_full_report.pdf. The National Institute of Standards and Technology (NIST) has identified five essential characteristics of cloud computing: on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service. Peter Mell and Tim Gance, *The NIST Definition of Cloud Computing*, version 15, Oct. 7, 2009, <http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc>.

7. Recently, identity theft alone was estimated to cause economic losses of more than \$15 billion in a single year. Fed. Trade Comm'n, *2006 Identity Theft Survey Report (2007)*, available at <http://www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf>.

The comprehensive consumer data privacy framework set forth here will provide clearer protections for consumers. It will also provide greater certainty for companies while promoting innovation and minimizing compliance costs (consistent with the goals of Executive Order 13563, "Improving Regulation and Regulatory Review"). The framework provides consumers who want to understand and control how personal data flows in the digital economy with better tools to do so. The proposal ensures that companies striving to meet consumers' expectations have more effective ways of engaging consumers and policymakers. This will help companies to determine which personal data practices consumers find unobjectionable and which ones they find invasive. Finally, the Administration's consumer data privacy framework improves our global competitiveness by promoting international policy frameworks that reflect how consumers and companies actually use networked technologies.

As a world leader in Internet innovation, the United States has both the responsibility and incentive to help establish forward-looking privacy policy models that foster innovation and preserve basic privacy rights. The Administration's framework for consumer data privacy offers a path toward achieving these goals. It is based on the following key elements:

- **A Consumer Privacy Bill of Rights**, setting forth individual rights and corresponding obligations of companies in connection with personal data. These consumer rights are based on U.S.-developed and globally recognized Fair Information Practice Principles (FIPPs), articulated in terms that apply to the dynamic environment of the Internet age;
- **Enforceable codes of conduct**, developed through **multistakeholder processes**, to form the basis for specifying what the Consumer Privacy Bill of Rights requires in particular business contexts; *industry specific*
- Federal Trade Commission (FTC) **enforcement** of consumers' data privacy rights through its authority to prohibit unfair or deceptive acts or practices; and
- Increasing **global interoperability** between the U.S. consumer data privacy framework and other countries' frameworks, through mutual recognition, the development of codes of conduct through multistakeholder processes, and enforcement cooperation can reduce barriers to the flow of information.

Consumer Data Privacy in a Networked World builds on the recommendations of the Department of Commerce Internet Policy Task Force's December 2010 report, *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework* ("Privacy and Innovation Green Paper").⁸ The Internet Policy Task Force developed the recommendations in the Privacy and Innovation Green Paper by engaging with stakeholders—companies, trade groups, privacy advocates, academics, State Attorneys General, Federal civil and criminal law enforcement representatives, and international partners—through a public symposium, written comments, public speeches and presentations, and informal meetings. More than 100 stakeholders subsequently submitted written comments on the Privacy and Innovation Green Paper. These comments provided the Administration with invaluable feedback during the development of *Consumer Data Privacy in a Networked World*. The Administration gratefully acknowledges the time and resources stakeholders devoted to this issue. Their ongoing engagement will be critical to implementing the framework successfully.

8. Department of Commerce, *Commercial Data Privacy and Innovation in the Internet Economy: Dynamic Policy Framework*, Dec. 2010, available at <http://www.ntia.doc.gov/report/2010/commercial-data-privacy-and-innovation-internet-economy-dynamic-policy-framework>.



II. Defining a Consumer Privacy Bill of Rights

Strengthening consumer data privacy protections and promoting innovation require privacy protections that are comprehensive, actionable, and flexible. The United States pioneered the FIPPs in the 1970s, and they have become the globally recognized foundations for privacy protection. The United States has embraced FIPPs by incorporating them into sector-specific privacy laws and applying them to personal data that Federal agencies collect. FIPPs also are a foundation for numerous international data privacy frameworks.⁹ These principles continue to provide a solid foundation for consumer data privacy protection, despite far-reaching changes in companies' ability to collect, store, and analyze personal data.

Should read
The Consumer Privacy Bill of Rights applies FIPPs to an environment in which processing of data about individuals is far more decentralized and pervasive than it was when FIPPs were initially developed. Large corporations and government agencies collecting information for relatively static databases are no longer typical of personal data collectors and processors. The world is far more varied and dynamic. Companies process increasing quantities of personal data for a widening array of purposes. Consumers increasingly exchange personal data in active ways through channels such as online social networks and personal blogs. The reuse of personal data can be an important source of innovation that brings benefits to consumers but also raises difficult questions about privacy. The central challenge in this environment is to protect consumers' privacy expectations while providing companies with the certainty they need to continue to innovate.¹⁰

To meet this challenge, the Consumer Privacy Bill of Rights carries FIPPs forward in two ways. First, it affirms a set of consumer rights that inform consumers of what they should expect of companies that handle personal data. The Consumer Privacy Bill of Rights also recognizes that consumers have certain responsibilities to protect their privacy as they engage in an increasingly networked society. Second, the Consumer Privacy Bill of Rights reflects the FIPPs in a way that emphasizes the importance of context in their application.¹¹ Key elements of context include the goals or purposes that consumers can expect

9. As noted in the Privacy and Innovation Green Paper (p. 11):

In 1973, the Department of Health, Education, and Welfare (HEW) released its report, *Records, Computers, and the Rights of Citizens*, which outlined a Code of Fair Information Practices that would create "safeguard requirements" for certain "automated personal data systems" maintained by the Federal Government. This Code of Fair Information Practices, now commonly referred to as fair information practice principles (FIPPs), established the framework on which much privacy policy would be built.

Examples of FIPPs-based international frameworks include the Organisation for Economic Co-operation and Development *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* and the Asia-Pacific Economic Cooperation *Privacy Framework*. The Privacy and Innovation Green Paper proposed for consideration the following set of FIPPs: transparency, individual participation, purpose specification, data minimization, use limitation, data quality and integrity, security, and accountability and auditing.

10. As the Privacy and Innovation Green Paper noted, "New devices and applications allow the collection and use of personal information in ways that, at times, can be contrary to many consumers' privacy expectations." Department of Commerce, Privacy and Innovation Green Paper, at i (statement of Commerce Secretary Gary Locke).

11. For a comparison of the Consumer Privacy Bill of Rights to other statements of the FIPPs, see Appendix B.

CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING
PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY

to achieve by using a company's products or services, the services that the companies actually provide, the personal data exchanges that are necessary to provide these services, and whether a company's customers include children and adolescents. Context should shape the balance and relative emphasis of particular principles in the Consumer Privacy Bill of Rights.

The Consumer Privacy Bill of Rights advances these objectives by holding that consumers have a right to:

- Individual Control
 - Transparency
 - Respect for Context
 - Security
 - Access and Accuracy
 - Focused Collection
 - Accountability
- 

The Consumer Privacy Bill of Rights applies to commercial uses of personal data. This term refers to any data, including aggregations of data, which is linkable to a specific individual.¹² Personal data may include data that is linked to a specific computer or other device. For example, an identifier on a smartphone or family computer that is used to build a usage profile is personal data. This definition provides the flexibility that is necessary to capture the many kinds of data about consumers that commercial entities collect, use, and disclose.

The remainder of this section provides the full statement of the Consumer Privacy Bill of Rights and explains the rationale for the rights and obligations under each principle.

12. This definition is similar to the Federal Government's definition of "personally identifiable information":

[I]nformation that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified.

Peter R. Orszag, Memorandum for the Heads of Executive Departments and Agencies, Guidance for Agency Use of Third-Party Websites and Applications, at 8 (Appendix), June 25, 2010, http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-23.pdf.

II. DEFINING A CONSUMER PRIVACY BILL OF RIGHTS

- Very flexible standard*
1. **Individual Control:** Consumers have a right to exercise control over what personal data companies collect from them and how they use it. Companies should provide consumers appropriate control over the personal data that consumers share with others and over how companies collect, use, or disclose personal data. Companies should enable these choices by providing consumers with easily used and accessible mechanisms that reflect the scale, scope, and sensitivity of the personal data that they collect, use, or disclose, as well as the sensitivity of the uses they make of personal data. Companies should offer consumers clear and simple choices, presented at times and in ways that enable consumers to make meaningful decisions about personal data collection, use, and disclosure. Companies should offer consumers means to withdraw or limit consent that are as accessible and easily used as the methods for granting consent in the first place.
- market for data*

The Individual Control principle has two dimensions. First, at the time of collection, companies should present choices about data sharing, collection, use, and disclosure that are appropriate for the scale, scope, and sensitivity of personal data in question. For example, companies that have access to significant portions of individuals' Internet usage histories, such as search engines, ad networks, and online social networks, can build detailed profiles of individual behavior over time. These profiles may be broad in scope and large in scale, and they may contain sensitive information, such as personal health or financial data.¹³ In these cases, choice mechanisms that are simple and prominent and offer fine-grained control of personal data use and disclosure may be appropriate. By contrast, services that do not collect information that is reasonably linkable to individuals may offer accordingly limited choices.

Should read white paper

In any event, a company that deals directly with consumers should give them appropriate choices about what personal data the company collects, irrespective of whether the company uses the data itself or discloses it to third parties. When consumer-facing companies contract with third parties that gather personal data directly from consumers (as is the case with much online advertising), they should be diligent in inquiring about how those third parties use personal data and whether they provide consumers with appropriate choices about collection, use, and disclosure. The Administration also encourages consumer-facing companies to act as stewards of personal data that they and their business partners collect from consumers. Consumer-facing companies should seek ways to recognize consumer choices through mechanisms that are simple, persistent, and scalable from the consumer's perspective.

for more at all -> clickstream

Third parties should also offer choices about personal data collection that are appropriate for the scale, scope, and sensitivity of data they collect. The focal point for much of the debate about third-party personal data collection in recent years is online behavioral advertising—the practice of collecting

13. "Scope" refers to the range of activities or interests as well as the time period that is reflected in a dataset. "Scale" refers to the number of individuals whose activities are in a dataset.

information about consumers' online interests in order to deliver targeted advertising to them.¹⁴ This system of advertising revolves around ad networks that can track individual consumers—or at least their devices—across different websites. When organized according to unique identifiers, this data can provide a potentially wide-ranging view of individual use of the Internet. These individual behavioral profiles allow advertisers to target ads based on inferences about individual interests, as revealed by Internet use. Targeted ads are generally more valuable and efficient than purely contextual ads and provide revenue that supports an array of free online content and services.¹⁵ However, many consumers and privacy advocates find tracking and the advertising practices that it enables invade their expectations of privacy.¹⁶

The Administration recognizes that the ultimate uses of personal data that third parties, such as ad networks, collect affect the privacy interests at stake. As a result, these uses of personal data should help to shape the range of appropriate individual control options. For example, a company that uses personal data only to calculate statistics about how consumers use its services may not implicate significant consumer privacy interests and may not need to provide consumers with ways to prevent data collection for this purpose. Even if the company collects and stores some personal data for some uses, it may not need to provide consumers with a sophisticated array of choices about collection. In the case of online advertising, for instance, verifying ad delivery and preventing a consumer from seeing the same ad many times over may require some personal data collection. But personal data collected only for these statistical purposes may not require the assembly of extensive, long-lived individual profiles and may not require extensive options for control.

Innovative technology can help to expand the range of user control. It is increasingly common for Internet companies that have direct relationships with consumers to offer detailed privacy settings that allow individuals to exercise greater control over what personal data the companies collect, and when. In addition, privacy-enhancing technologies such as the "Do Not Track" mechanism allow consumers to exercise some control over how third parties use personal data or whether they receive it at all. For example, prompted by the FTC,¹⁷ members of the online advertising industry developed self-regulatory principles based on the FIPPs, a common interface to alert consumers of the presence of third party ads and to direct them to more information about the relevant ad network, and a common mechanism to

14. See FTC, *Self-Regulatory Principles for Online Behavioral Advertising* (staff report), at 2, Feb. 2009 (stating that online behavioral advertising "involves the tracking of consumers' online activities in order to deliver tailored advertising").

15. According to one study, behaviorally targeted ads are worth significantly more than non-targeted ads. See Howard Beales, *The Value of Behavioral Targeting*, at 3, Mar. 24, 2010 (finding, based on data provided by ad networks, that behaviorally targeted ad rates in 2009 were 2.68 times greater than non-targeted ad rates), http://www.networkadvertising.org/pdfs/Beales_NAI_Study.pdf; FTC, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers* (preliminary staff report), at 24, Dec. 2010 (reporting that FTC privacy roundtable participants discussed that "the more information that is known about a consumer, the more a company will pay to deliver a precisely-targeted advertisement to him") ("FTC Staff Report").

16. See Aleecia M. McDonald and Lorrie Faith Cranor, *Americans' Attitudes About Internet Behavioral Advertising Practices*, Proceedings of the 9th Annual ACM Workshop on Privacy in the Electronic Society (WPES) (2010).

17. See generally FTC, *Self-Regulatory Principles for Online Behavioral Advertising* (staff report), Feb. 2009.

II. DEFINING A CONSUMER PRIVACY BILL OF RIGHTS

allow consumers to opt out of targeted advertising by individual ad networks.¹⁸ A variety of other actors, including browser vendors, software developers, and standards-setting organizations, are developing “Do Not Track” mechanisms that allow consumers to exercise some control over whether third parties receive personal data. All of these mechanisms show promise. However, they require further development to ensure they are easy to use, strike a balance with innovative uses of personal data, take public safety interests into account, and present consumers with a clear picture of the potential costs and benefits of limiting personal data collection.

As third parties become further removed from direct interactions with consumers, it may be more difficult for them to provide consumers with meaningful control over data collection. Data brokers, for example, aggregate personal data from multiple sources, often without interacting with consumers at all. Such companies face a challenge in providing effective mechanisms for individual control because consumers might not know that these third parties exist. Moreover, some data brokers collect court records, news reports, property records, and other data that is in the public record. The rights of freedom of speech and freedom of the press involved in the collection and use of these documents must be balanced with the need for transparency to individuals about how data about them is collected, used, and disseminated and the opportunity for individuals to access and correct data that has been collected about them.

Still, data brokers and other companies that collect personal data without direct consumer interactions or a reasonably detectable presence in consumer-facing activities should seek innovative ways to provide consumers with effective Individual Control. If it is impractical to provide Individual Control, these companies should ensure that they implement other elements of the Consumer Privacy Bill of Rights in ways that adequately protect consumers’ privacy. For example, to provide sufficient privacy protections, such companies may need to go to extra lengths to implement other principles such as Transparency—by providing clear, public explanations of the roles they play in commercial uses of personal data—as well as providing appropriate use controls once information is collected under the Access and Accuracy and Accountability principles to compensate for the lack of a direct consumer relationship.

The second dimension of Individual Control is consumer responsibility. In a growing number of cases, such as online social networks, the use of personal data begins with individuals’ decisions to choose privacy settings and to share personal data with others. In such contexts, consumers should evaluate their choices and take responsibility for the ones that they make. Control over the initial act of sharing is critical. Consumers should take responsibility for those decisions, just as companies that participate in and benefit from this sharing should provide usable tools and clear explanations to enable consumers to make meaningful choices.

The Individual Control principle also recognizes that consumers’ privacy interests in personal data persist throughout their relationships with a company. Accordingly, this principle includes a right to withdraw consent to use personal data that the company controls. Companies should provide means of with-

18. See AboutAds.info, *Self-Regulatory Principles for Online Behavioral Advertising*, <http://www.aboutads.info/resource/download/seven-principles-07-01-09.pdf> (July 2009); Interactive Advertising Bureau, Comment on the Privacy and Innovation Green Paper (Attachment B) (explaining online advertisers’ system for directing users to ad networks’ privacy policies and opt-outs).

drawing consent that are on equal footing with ways they obtain consent. For example, if consumers grant consent through a single action on their computers, they should be able to withdraw consent in a similar fashion.¹⁹

There are three practical limits to the right to withdraw consent. First, it presumes that consumers have an ongoing relationship with a company. This relationship could be minimal, such as a consumer establishing an account for a single transaction; or it may be as extensive as many financial transactions spanning many years. Nonetheless, the company must have a way to effect a withdrawal of consent to the extent the company has associated and retained data with an individual. Conversely, data that a company cannot reasonably associate with an individual is not subject to the right to withdraw consent. Second, the obligation to respect a consumer's withdrawal of consent only extends to data that the company has under its control. Third, the Individual Control principle does not call for companies to permit withdrawal of consent for personal data that they collected before implementing the Consumer Privacy Bill of Rights, unless they made such a commitment at the time of collection.

2. **TRANSPARENCY:** Consumers have a right to easily understandable and accessible information about privacy and security practices. At times and in places that are most useful to enabling consumers to gain a meaningful understanding of privacy risks and the ability to exercise Individual Control, companies should provide clear descriptions of what personal data they collect, why they need the data, how they will use it, when they will delete the data or de-identify it from consumers, and whether and for what purposes they may share personal data with third parties.

Plain language statements about personal data collection, use, disclosure, and retention help consumers understand the terms surrounding commercial interactions. Companies should make these statements visible to consumers when they are most relevant to understanding privacy risks and easily accessible when called for.

Personal data uses that are not consistent with the context of a company-to-consumer transaction or relationship deserve more prominent disclosure than uses that are integral to or commonly accepted in that context. Privacy notices that distinguish personal data uses along these lines will better inform consumers of personal data uses that they have not anticipated, compared to many current privacy notices that generally give equal emphasis to all potential personal data uses.²⁰ Such notices will give privacy-conscious consumers easy access to information that is relevant to them. They may also promote greater consistency in disclosures by companies in a given market and attract the attention of consumers who ordinarily would ignore privacy notices, potentially making privacy practices a more salient point of competition among different products and services.

19. The obligation to provide these choices should be read in conjunction with the Access and Accuracy principle discussed below.

20. See Assistant Secretary for Communications and Information Lawrence E. Strickling, Testimony Before the Senate Committee on Commerce, Science, and Transportation, Mar. 16, 2011, at 2-3.

II. DEFINING A CONSUMER PRIVACY BILL OF RIGHTS

In addition, companies should provide notice in a form that is easy to read on the devices that consumers actually use to access their services. In particular, mobile devices have small screens that make reading full privacy notices effectively impossible. Companies should therefore strive to present mobile consumers with the most relevant information in a manner that takes into account mobile device characteristics, such as small display sizes and privacy risks that are specific to mobile devices.

Finally, companies that do not interact directly with consumers—such as the data brokers discussed above—need to make available explicit explanations of how they acquire, use, and disclose personal data. These companies may need to compensate for the lack of a direct relationship when making these explanations available, for example by posting them on their websites or other publicly accessible locations. Moreover, companies that have first-party relationships with consumers should disclose specifically the purpose(s) for which they provide personal data to third parties, help consumers to understand the nature of those third parties' activities, and whether those third parties are bound to limit their use of the data to achieving those purposes. This gives consumers a more tractable task of assessing whether to engage with a single entity, rather than trying to understand what personal data third parties—potentially dozens, or even hundreds—receive and how they use it. Similarly, first parties could create greater transparency by disclosing what kinds of personal data they obtain from third parties, who the third parties are, and how they use this data. This level of transparency may also facilitate the development within the private sector of innovative privacy-enhancing technologies and guidance that consumers can use to protect their privacy.

3. **RESPECT FOR CONTEXT:** Consumers have a right to expect that companies will collect, use, and disclose personal data in ways that are consistent with the context in which consumers provide the data. Companies should limit their use and disclosure of personal data to those purposes that are consistent with both the relationship that they have with consumers and the context in which consumers originally disclosed the data, unless required by law to do otherwise. If companies will use or disclose personal data for other purposes, they should provide heightened Transparency and Individual Choice by disclosing these other purposes in a manner that is prominent and easily actionable by consumers at the time of data collection. If, subsequent to collection, companies decide to use or disclose personal data for purposes that are inconsistent with the context in which the data was disclosed, they must provide heightened measures of Transparency and Individual Choice. Finally, the age and familiarity with technology of consumers who engage with a company are important elements of context. Companies should fulfill the obligations under this principle in ways that are appropriate for the age and sophistication of consumers. In particular, the principles in the Consumer Privacy Bill of Rights may require greater protections for personal data obtained from children and teenagers than for adults.

Respect for Context distinguishes personal data uses on the basis of how closely they relate to the purposes for which consumers use a service or application as well as the business processes necessary to provide the service or application.²¹ The Respect for Context principle calls on companies that collect data to act as stewards of data in ways that respect their consumers. This principle derives from two principles commonly found in statements of the FIPPs. The first principle, purpose specification, states that companies should specify at the time of collection the purposes for which they collect personal data. Second, the use limitation principle holds that companies should use personal data only to fulfill those specific purposes.

The Respect for Context principle adapts these well-established principles in two ways. First, Respect for Context provides a substantive standard to guide companies' decisions about their basic personal data practices. Generally speaking, companies should limit personal data uses to fulfilling purposes that are consistent with the context in which consumers disclose personal data. Second, while this principle emphasizes the importance of the relationship between a consumer and a company at the time consumers disclose data, it also recognizes that this relationship may change over time in ways not foreseeable at the time of collection. Such adaptive uses of personal data may be the source of innovations that benefit consumers. However, companies must provide appropriate levels of transparency and individual choice—which may be more stringent than was necessary at the time of collection—before reusing personal data.

Applying the Consumer Privacy Bill of Rights in a context-specific manner provides companies flexibility but also requires them to consider carefully what consumers are likely to understand about their data practices based on the products and services they offer, how the companies themselves explain the roles of personal data in delivering them, research on consumers' attitudes and understandings, and feedback from consumers. Context should help to determine which personal data uses are likely to raise the greatest consumer privacy concerns. The company-to-consumer relationship should guide companies' decisions about which uses of personal data they will make most prominent in privacy notices. For

21. Several commenters on the Privacy and Innovation Green Paper emphasized the importance of context in applying FIPPs. See, e.g., AT&T Comment on the Privacy and Innovation Green Paper, at 7, Jan. 28, 2011 ("FIPPs are usefully expressed as generalized policy guides that should shape the multi-stakeholder collaborative processes to develop flexible and contextualized codes of practice for particular industries."); Centre for Information Policy Leadership Comment on the Privacy and Innovation Green Paper, at 3, Jan. 28, 2011 ("Principles of fair information practices should be applied within a contextual framework, and not in a rigid or fixed way."); Google Comment on the Privacy and Innovation Green Paper, at 6, Jan. 28, 2011 ("In particular, FIPPs must be flexible enough to take account of the spectrum of identifiability, linkability, and sensitivity of various data in various contexts."); Intel Comment on the Privacy and Innovation Green Paper, at 4 ("[M]any of the issues present in a privacy regulatory scheme are highly contextual."); Intuit Comment on the Privacy and Innovation Green Paper, at 9 ("It is the use of the information as well as its characteristics that should inform our treatment of it. Context is crucial."); Helen Nissenbaum, Kenneth Farrall, and Finn Brunton, Comment on the Privacy and Innovation Green Paper, at 2-3 (recommending consideration of context as a source of "baseline substantive constraints on data practices following the model of current US sectoral privacy regulation"); Online Publishers Association Comment on the Privacy and Innovation Green Paper, at 6 ("Online publishers share a direct and trusted relationship with visitors to their sites. In the context of this relationship, OPA members sometimes collect and use information to target and deliver the online advertising that subsidizes production of quality digital content."); TRUSTe Comment on the Privacy and Innovation Green Paper, at 2 ("We view privacy as inherently contextual; disclosure obligations will differ depending on the context of the interaction."). Current scholarship also emphasizes the importance of the relationship between context and privacy. See Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (2009).