“Respect for context” in privacy online

Helen Nissenbaum
New York University

Symposium on Internet Privacy
A culture of privacy and trust on the Internet

acatech NATIONAL ACADEMY OF SCIENCE & ENGINEERING
BERLIN 3.26.12

Research supported by US-AFSOR: ONR BAA 07-03 (MURI) and US NSF CT-M: Privacy, Compliance, & Information Risk CNS-0831124
IN THE NEWS

EU fights ‘fierce lobbying’ to devise data privacy law
It’s in demand, but a new EU privacy law aims to return control of personal details to you.

Supreme Court Deals Blow To Government Surveillance, Saying Warrant Needed For GPS

Watchdog sues FTC over new Google privacy policy
Rather than take on Google, the Electronic Privacy Information Center is asking the court to block new information sharing and force federal regulators to protect Google users.

Don’t Forgive Path, the Creepy iPhone Company that Misled Us Once Already
A CONSUMER INTERNET PRIVACY
BILL OF RIGHTS

The Obama Administration believes America must apply our timeless privacy values to the new technologies and circumstances of our times. Citizens are entitled to have their personal data handled according to these principles.

Individual Control
Consumers have a right to exercise control over what personal data companies collect from them and how they use it.

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 and risk associated with the data.

Transparency
Consumers have a right to easily understandable and accessible information about privacy and security practices.

Focused Collection
Consumers have a right to reasonable limits on the personal data that companies collect and retain.

Respect for Context
Consumers have a right to expect that companies will collect, use, and disclose personal data in ways that are consistent.

Accountability
Companies should be accountable to enforcement authorities and consumers for adhering to these principles.

Security
Consumers have a right to secure and responsible handling of personal data.

Feb 23, 2012
White House announces Privacy Bill of Rights
Privacy worries online

• Surreptitious 3rd parties (e.g. ad networks)
  • Beacons
  • Cookies
  • Flash cookies
• 3rd party intermediaries (e.g. Facebook)
• 2nd parties (e.g. Amazon, The New York Times)

Technical affordance vs. public moral & political imperative
STRAWBERRY RHUBARB CRISP WITH OAT PECAN CRUMB

Tell us what matters and make your voice heard. safecount.net
Japan Nuke Plant Operator Missteps

The operator of the stricken Japan nuclear plant faces government criticism after ignoring key safety measures, including sending workers in without protective footwear.

- Radioactive Water Found Near Plant
- U.S. Navy Tries to Douse Nuke Crisis
- PHOTOS: Japan Aftermath
- VIDEO: Breach at Reactor Core?
- Faults Uncovered in U.S. Radiation Monitoring System

Woman Claims She Was Raped by Libyan Troops

Mom Claims Son Died Losing Weight For Army

First Woman VP Nominee Geraldine Ferraro Dies

Woman sets off brawl after storming into Tripoli hotel to tell reporters

An Ohio mom blames her son's death on Army recruiters, who she claims

The first woman to run for vice president and Fox News contributor

MARKETS

<table>
<thead>
<tr>
<th>Index</th>
<th>Value</th>
<th>Change</th>
<th>Gain/loss</th>
</tr>
</thead>
<tbody>
<tr>
<td>DJIA</td>
<td>12,220.59</td>
<td>+50.03</td>
<td>+0.41%</td>
</tr>
<tr>
<td>Nasdaq</td>
<td>2,743.06</td>
<td>+6.64</td>
<td>+0.24%</td>
</tr>
<tr>
<td>S&amp;P 500</td>
<td>1,912.80</td>
<td>+4.14</td>
<td>+0.22%</td>
</tr>
</tbody>
</table>

Get $125
Technical mediation of privacy threats

- GPS, mobile, implantable devices
- RFID, “emanations”
- Biometrics
- Pervasive sensory networks
- Networked video and audio capture
- Web cookies, flash cookies, web bugs
- Databases, storage, retrieval
- Information aggregation, mining, profiling
- “Big data,” evidence based everything
- The Internet, the Web
- Social computing, Web 2.0
- Email, mobile media
The worry about IT and privacy

• Control
• Quantity
Protecting online privacy

Currently predominant

Transparency (notice) and choice (consent)

Implemented as “voluntary, enforceable privacy policies”
Privacy Policy

Last modified: March 1, 2012 (view archived versions)

There are many different ways you can use our services – to search for and share information, to communicate with other people or to create new content. When you share information with us, for example by creating a Google Account, we can make those services even better – to show you more relevant search results and ads, to help you connect with people or to make sharing with others quicker and easier. As you use our services, we want you to be clear how we’re using information and the ways in which you can protect your privacy.

Our Privacy Policy explains:

Transparency and choice
People have different privacy concerns. Our goal is to be clear about what information we collect, so that you can make meaningful choices about how it is used. For example, you can:

- Review and control certain types of information tied to your Google Account by using Google Dashboard.
- View and edit your ads preferences, such as which categories might interest you, using the Ads Preferences Manager. You can also opt out of certain Google advertising services here.
- Use our editor to see and adjust how your Google Profile appears to particular individuals.
- Control who you share information with.
- Take information out of many of our services.

You may also set your browser to block all cookies, including cookies associated with our services, or to indicate when a cookie is being set by us. However, it’s important to remember that many of our services may not function properly if your cookies are disabled. For example, we may not remember your language preferences.

Information you share
Many of our services let you share information with others. Remember that when you share information publicly, it may be indexable by search engines, including Google. Our services provide you with different options on sharing and removing your content.
Transparency & choice: why not?

- Hasn’t worked: status quo
- Poorly implemented (“critical adherents”)
- Transparency Paradox
Transparency & choice: why?

• Privacy as control
• Privacy as a preference
• Net as competitive free market
• Has worked elsewhere; will work online
• We can do better (Calo: “visceral notice”)
• What’s the alternative?
The worry about IT and privacy

- Control
- Quantity
- Appropriateness
Obtaining information
Monitoring, surveillance, capture, tracking ...

Utilizing information
Storage, aggregation, analysis, ...

Distributing information
Communication, dissemination, disclosure, ...

DISRUPTIVE INFORMATION FLOWS
The theory of contextual integrity
Contextual Integrity in brief

_a theory of privacy as appropriate flow_

- **Contexts**
  - structured spheres of social life characterized by canonical activities, practices, roles, norms, goals, values. (e.g. healthcare, education, personal and home-life, religion.)

- **Context-relative Informational norms**

- **Why informational norms matter**
  - This component of the theory addresses ethical and political legitimacy
Informational norms

In a job interview, the interviewer may not ask the candidate’s religious affiliation.

A priest may not divulge a congregant’s confession to anyone.

A citizen of the U.S. is obliged to reveal gross income to the IRS.
Informational norms: structure

Key Parameters

- **Actors**
  - Sender
  - Recipient
  - Subject

- **Information types**
  - Demographic, biographical
  - Actions, communications
  - Medical status, financial

- **Transmission Principles**
  - Consent, coerce, steal, buy, sell
  - Confidentially, fiduciary, with a warrant, surreptitiously

**E.g.**
- Physician, merchant, bank, friend
- Merchant, police, ad network
- Patient, shopper, investor, reader
A common mistake

Failure to specify a key parameter

Actors
- Sender
- Recipient
- Subject
Contextual integrity is breached when actions or practices violate informational norms
Why respect contexts, norms?

Sustain general moral and political values
- prevent harm and risk
- limit unfair discrimination
- support freedoms
- promote autonomy

**Privacy beyond harm**

Context specific, internal values, ends, purposes
- medical: health; nondiscrimination
- educational: intellectual growth; just dessert
- political: democracy
- home and social: trust, autonomy, stability
“While the government does not know every source of income of a taxpayer and must rely upon the good faith of those reporting income, still in the great majority of cases this reliance is entirely justifiable, principally because the taxpayer knows that in making a truthful disclosure of the sources of his income, information stops with the government. It is like confiding in one’s lawyer.”

Secretary of the Treasury, Andrew Mellon, 1925
“Cyberspace” ...
media space
not autonomous, virgin territory

Wells Fargo online, Zappos, IRS.gov
E*Trade, WebMD, LexisNexis, Craig’s list, email
Google Search, MMORGs, Delicious, blogs

Deeply integrated
Radically heterogeneous
“Respect for contexts” online

Contexts not political economy
Contexts not platforms
One policy, one Google experience

We're getting rid of over 60 different privacy policies across Google and replacing them with one that's a lot shorter and easier to read. Our new policy covers multiple products and features, reflecting our desire to create one beautifully simple and intuitive experience across Google.

This stuff matters, so please take a few minutes to read our updated Google Privacy Policy and Terms of Service now. These changes will take effect on March 1, 2012.

Easy to work across Google

Our new policy reflects our desire to create a simple product experience that does what you need, when you want it to. Whether you're reading an email that reminds you to schedule a family get-together or finding a favorite video that you want to share, we want to ensure you can move across Gmail, Calendar, Search, YouTube, or whatever your life calls for with ease.

Tailored for you

If you're signed into Google, we can do things like suggest search queries -- or tailor your search results -- based on the interests you've expressed in Google+, Gmail, and YouTube. We'll better understand which version of Pink or Jaguar you're searching for and get you those results faster.

Easy to share and collaborate

When you post or create a document online, you often want others to see and contribute. By remembering the contact information of the people you want to share with, we make it easy for you to share in any Google product or service with minimal clicks and errors.

Protecting your privacy hasn't changed

Our goal is to provide you with as much transparency and choice as possible, through products like Google Dashboard and Ads Preferences Manager alongside other tools. Our privacy principles remain unchanged. And we'll never sell your personal information or share it without your permission (other than rare circumstances like valid legal requests).

Understand how Google uses your data

If you want to learn more about your data on Google and across the web, including tips and advice for staying safe online, check out Good to Know.

Got questions? We've got answers

Visit our FAQ to read more about the changes. (We figured our users might have a question or twenty-two.)

Notice of change

March 1, 2012 is when the new Privacy Policy and Google Terms of Service will come into effect. If you choose to keep using Google once the change occurs, you will be doing so under the new Privacy Policy and Terms of Service.
Respecting contexts online

- Locate and respect substantive informational norms
  - Call yourself a church, university, information provider, health information repository, video delivery service
  - Assert entrenched rule-sets
- Reveal the unexpected
- Conduct evaluations for disruptive or novel flow patterns
  - Test new practices against ethical and political values and internal standards (values, ends, purposes);
  - Aspire to context-specific standards of excellence
- Seek permission for grey areas (role for T&P)
"A Contextual Approach to Privacy Online"

*Daedalus* 140 (4) (Fall 2011)
When patients share health information with physicians, physicians may share it with other healthcare providers only if it serves the patients' direct health interests.

Financial institutions must notify consumers if they share their non-public personal information with non-affiliated companies, but the notification may occur either before or after the information sharing occurs.

Transmission principle

In our formal computer language,

\( \forall p_1, p_2, q : P. \forall m : M. \forall t : T. \)

\( \incontext(p_1, c) \land \send(p_1, p_2, m) \land \contains(m, q, t) \rightarrow \)

\( \inrole(p_1, institution) \land \inrole(p_2, non-affiliate) \land \inrole(q, consumer) \land (t \in npi) \rightarrow \)

\( \Box \send(p_1, q, privacy-notice) \lor \Box \send(p_1, q, privacy-notice) \)