Privacy Matters
and why you shouldn’t “get over it”

Winter 2016

Overview
● What is Privacy?
● Value of Privacy
● History of Privacy
● Privacy & Security
● Focus: Privacy & Big Data
● Parting Thoughts
● Resources
What is Privacy?

Privacy Is In The News

Big Data and the Underground Railroad

Game for privacy is gone, mass surveillance is here to stay

Don't breach encryption warns privacy watcher

Internet providers want to know more about you than Google does, privacy groups say

Since when was your privacy a commodity?

Turning Tech Companies Into Spies Won't Work

Big data and transparency: Why it matters to you

There Is No Privacy On The Internet Of Things
What the Experts Say (1890-1977)

**1890.** Recent inventions ... call attention to the next step which must be taken for the protection of the person, and for securing to the individual ... the right to be let alone. *(Samuel Warren & Louis D. Brandeis)*

**1890.** Privacy is the right to be alone—the most comprehensive of rights, and the right most valued by civilized man. *(Louis D. Brandeis)*

**1967.** Privacy is the right of individuals to control, edit, manage, and delete information about themselves, and to decide when, how, and to what extent information is communicated to others. *(Alan Westin)*

**1977.** Building and maintaining an enduring, intimate relationship is a process of privacy regulation. *(Irwin Altman)*


**1999.** You have zero privacy anyway. Get over it. *(Scott McNealy)*

**2001.** Privacy is necessary to protect citizens from the misjudgments that can result from the exposure of too much information as well as too little information. *(Jeffrey Rosen)*

**2010.** People have really gotten comfortable not only sharing more information and different kinds, but more openly and with more people—and that social norm [privacy] is just something that has evolved over time. *(Mark Zuckerberg)*

**2015.** Arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say. *(Edward Snowden)*
What is Privacy?

What the Public Says

Three-year study showed that the more people disclosed about themselves on social media, the more privacy they said they desired.

-Pew Research 2014

The Value of Privacy

Privacy is Tied to Liberty, Ethics, & Compliance

<table>
<thead>
<tr>
<th>Civil Liberties</th>
<th>Freedom of thought, speech, expression</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Freedom of social and political activities</td>
</tr>
<tr>
<td></td>
<td>Freedom of association</td>
</tr>
<tr>
<td></td>
<td>Limits authority</td>
</tr>
<tr>
<td>Individual Liberties</td>
<td>Promotes individuality</td>
</tr>
<tr>
<td></td>
<td>Ability to grow and change</td>
</tr>
<tr>
<td></td>
<td>Autonomy and control over self</td>
</tr>
<tr>
<td></td>
<td>Allows for ability to reveal as much or as little about self</td>
</tr>
<tr>
<td>Ethics &amp; Respect</td>
<td>● Promotes ethical and respectful treatment of others</td>
</tr>
<tr>
<td>Compliance</td>
<td>● FERPA, HIPAA, GLBA, COPPA, etc...</td>
</tr>
</tbody>
</table>
### Value of Privacy (who didn’t have it)

<table>
<thead>
<tr>
<th>Country</th>
<th>Institution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Germany</td>
<td>Hitler’s Gestapo</td>
</tr>
<tr>
<td>USSR</td>
<td>Stalin’s (et al) KGB</td>
</tr>
<tr>
<td>East Germany</td>
<td>Honecker’s Stasi</td>
</tr>
<tr>
<td>Portugal</td>
<td>Salazar’s PVDE/PIDE</td>
</tr>
<tr>
<td>Spain</td>
<td>Franco’s Secret Police</td>
</tr>
<tr>
<td>Argentina</td>
<td>Junta’s “Dirty War”</td>
</tr>
<tr>
<td>Chile</td>
<td>Pinochet’s DINA</td>
</tr>
</tbody>
</table>

### The Value of Privacy

#### Individuals Value Their Privacy

- 91% of American adults say that consumers have lost control over how personal information is collected and used by companies. —Pew Research, 2015
- 86% of internet users have tried to use the internet in ways to minimize the visibility of their digital footprints. 55% of internet users have taken steps to hide from specific people or organizations. —Pew Research, 2013

“"What we can and should demand is a reasonable amount of control over which information we choose to divulge, stringent restrictions on who has access to it, and regular opportunities to review and correct it.” —Detroit Free Press, 2014

- 60% of Android downloaders have chosen not to install an app when they discovered how much personal information the app required in order to use it. Separately, 43% have uninstalled an app for the same reason after initially downloading it.” —Pew Research, 2015

Many Americans say they might provide personal information, depending on the deal being offered and how much risk they face. —Pew Research, 2015
**Value of Privacy in Higher Ed**

**Fundamental Component**
- Privacy underpins the academic and intellectual freedoms that are key to the university's teaching, learning, research, and clinical mission.
- Provides a basis for an ethical and respectful workplace.
- Allows for student growth and development.
- Together with information security, it is critical to the university’s ability to be a good steward of the information entrusted to it by students, faculty, staff, and the community.

**History of Privacy**

**Brief Legal Overview (1789-1977)**

- **1789**: U.S. Constitution
- **1890**: Brandeis Right to Privacy Law Review Article
- **1948**: U.N. Declaration of Human Rights
- **1967**: Privacy and Freedom Book
- **1968**: Privacy Tort
- **1974**: Privacy Act of 1974
- **1977**: FERPA Student Privacy
- **1948**: Supreme Court Rulings Related to Privacy (1960s-70s)

**Supreme Court Rulings Related to Privacy (1960s-70s)**

- [Image of Supreme Court with text: Privacy? Pahl! Why bother if you've done nothing wrong?]
### Brief Legal Overview (1991-2011)

<table>
<thead>
<tr>
<th>Year</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>1991</td>
<td>HIPAA Health &amp; Medical Privacy</td>
</tr>
<tr>
<td>1995</td>
<td>EU Data Protection Directive</td>
</tr>
<tr>
<td>1996</td>
<td>COPPA Children’s Online Privacy</td>
</tr>
<tr>
<td>1998</td>
<td>GLBA Loan Info</td>
</tr>
<tr>
<td>1999</td>
<td>First Chief Counselor for Privacy in Fed Govt.</td>
</tr>
<tr>
<td>2003</td>
<td>State Data Breach Notification Laws</td>
</tr>
<tr>
<td>2010</td>
<td>Red Flags Identity Theft Protection</td>
</tr>
<tr>
<td>2012</td>
<td>Google implements EU “Right to be Forgotten”</td>
</tr>
</tbody>
</table>

### History of Privacy

<table>
<thead>
<tr>
<th>Then</th>
<th>Now</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cameras</td>
<td>Cellphone cameras, Google Glass, drones</td>
</tr>
<tr>
<td>News (periodic): print, radio, TV</td>
<td>News (pervasive): social media</td>
</tr>
<tr>
<td>Phones</td>
<td>Cellphones, tablets</td>
</tr>
<tr>
<td>You &amp; your home</td>
<td>Google Street View, geo-location (satellite, cars, mobile devices), data-mining, profiling</td>
</tr>
<tr>
<td>Disconnected devices</td>
<td>Connected devices: Internet of things, wi-fi, wearables, smart phones, thermostats, appliances, cars</td>
</tr>
<tr>
<td>Advertising: print, radio, TV</td>
<td>Advertising: marketing &amp; behavioral profiling, data collection and resale</td>
</tr>
<tr>
<td>Phone book, census, credit agencies</td>
<td>Big Data (used beyond purpose for collection, re-identifying aggregate data, profiling</td>
</tr>
<tr>
<td>Government surveillance: telephone wiretaps, tails</td>
<td>Government surveillance: NSA Internet tapping, location tracking, facial recognition, pervasive data collection, profiling</td>
</tr>
</tbody>
</table>
Aside: Privacy & Security

Privacy Is Different From Security

<table>
<thead>
<tr>
<th>Security</th>
<th>Privacy</th>
</tr>
</thead>
<tbody>
<tr>
<td>...protects from unwanted intruders</td>
<td>...allows for freedom to conceal or reveal</td>
</tr>
</tbody>
</table>

From the 2013 University of California privacy and information security initiative
Fun Fact!
Did you know that security is one of the cornerstones of Privacy’s Fair Information Practice Principles (FiPPs)

“Aside” Privacy & Security

Privacy & Big Data
Case Studies

- **Netflix (2010)**
  - Researchers were able to identify two people out of the nearly half million anonymized users whose movie ratings were released by Netflix. Able to identify their political leanings and sexual orientation.

- **Target (2012)**
  - Used a statistical model based on purchase history to send a pregnant teenage girl coupons for baby gear. Her father went to the local store angry that his teen daughter had received the coupons...he didn’t know she was pregnant.

- **MIT Research (2015)**
  - Found three data points were enough to identify an even larger percentage of people in a data set. Ex: someone with a copy of a receipt, an Instagram photo of you having coffee with friends, and a tweet about the phone you just bought — would have a 94 percent chance of extracting your credit card records from those of a million other people.

Concerns - Not just a difference in scale

- Aggregation of anonymous or de-identified personal data can result in the creation of identifiable data.
- Data may be used beyond the intended purposes for which it was originally collected.
- The widespread collection, analysis, and sharing of data may run counter to the words or spirit of existing privacy policies or the institutional culture.
- Traditional privacy protections & processes may not work.
- Predictive data does not always mean accurate data.
- Profiling made easy.
Key Components of FIPPS Difficult to Apply

- **Individual Participation**: Organizations should involve the individual in the process of using PII and, to the extent practicable, seek individual consent for the collection, use, dissemination, and maintenance of PII. Organizations should also provide mechanisms for appropriate access, correction, and redress regarding use of PII.
- **Purpose Specification**: Organizations should specifically articulate the authority that permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used.
- **Data Minimization**: Organizations should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s).
- **Use Limitation**: Organizations should use PII solely for the purpose(s) specified in the notice. Sharing PII should be for a purpose compatible with the purpose for which the PII was collected.
- **Data Quality and Integrity**: Organizations should, to the extent practicable, ensure that PII is accurate, relevant, timely, and complete.

What to Do: Plan & Transparency

- **Plan**
  - Make sure appropriate stakeholders, such as general counsel, data owners, data users, are engaged as part of the planning process.
  - Provide training and guidance to those accessing the data.

- **Be Transparent**
  - Provide policies and information that describe how data is being collected, how it is being used, and how privacy is being addressed.
  - Communicate the benefits of big data.
  - Limit your data collection what is necessary for the outcome sought; be judicious in the types and amount of data collected.
  - Avoid appearing to be a profiler. Be cognizant of the privacy controversies related to the NSA and private-sector data collection practices.
Privacy & Big Data

What to Do: R-E-S-P-E-C-T

- Respectfully Use the Data
  - Avoid identification. Use aggregate, anonymized or de-identified data when practical.
  - Respect the context. Avoid using data collected for one purpose for different purposes, without appropriate planning and transparency.
  - Consider sharing. When feasible, provide analytical information back to the “subject.”
  - Limit access. Not all data users need access to all the data. Develop processes that only share the appropriate data sets.
  - Resist profiling/Keep the human element in mind. Do not allow data to entirely tell the story or entirely drive decisions.

Privacy & Big Data

What to Do: Empowerment

- Empower the “Subject”
  - When appropriate and/or possible, ask for consent or opt-in mechanisms before collecting data.
  - When appropriate and/or possible, provide opportunities for the subject to opt-out of some of either the data collection or usage (opt-out should not be assumed to be unworkable).
  - Provide reasonable access to individual data for review and correction.
The White House Intelligentsia Say...

- "[t]he challenges to privacy arise because technologies collect so much data (e.g., from sensors in everything from phones to parking lots) and analyze them so efficiently (e.g., through data mining and other kinds of analytics) that it is possible to learn far more than most people had anticipated or can anticipate given continuing progress. These challenges are compounded by limitations on traditional technologies used to protect privacy (such as de-identification)...technology alone cannot protect privacy, and policy intended to protect privacy needs to reflect what is (and is not) technologically feasible."

  - President’s Council of Advisors on Science and Technology, Big Data and Privacy: A Technological Perspective

The Everyday Person Says...

- "If I want to disclose information about my child, my family, my socioeconomic status, I should be the one to decide, not the school...My kids are there to learn, not to be part of a data set."

  - Tools for Tailored Learning May Expose Students’ Personal Details (New York Times, August 30, 2015)
Asilomar Convention as a model*

- **Respect for the rights and dignity of learners.**
  - Data collection, retention, use, and sharing practices must be made transparent...and findings made publicly available, with essential protections for the privacy of individuals...Researchers and institutions should be especially vigilant with regard to the collection and use of identifiable...data, including considerations of the appropriate form and degree of consent.

- **Beneficence.**
  - Individuals and organizations...have an obligation to maximize possible benefits while minimizing possible harms.

- **Continuous consideration.**
  - In a rapidly evolving field there can be no last word on ethical practice. Ethically responsible learner research requires ongoing and broadly inclusive discussion of best practices and comparable standards among researchers, learners, and educational institutions.

*For more on the Asilomar Convention and its tenets and principles - [http://asilomar-highered.info/](http://asilomar-highered.info/)

---

**Some Parting Thoughts**  
(or why privacy still matters)

- **1640.** If you give me six lines written by the hand of the most honest of men, I will find something in them which will hang him. *(attributed to Cardinal Richelieu)*

- **1966.** Everyone is guilty of something or has something to conceal. All one has to do is look hard enough to find what it is. *(Aleksandr Solzhenitsyn)*

- **1977.** The real danger is the gradual erosion of individual liberties through automation, integration, and interconnection of many small, separate record-keeping systems, each of which alone may seem innocuous, even benevolent, and wholly justifiable. *(U. S. Privacy Study Commission)*

- **1996.** Freedom is impossible in a society that refuses to respect the fact that “we act different in private than in public.” *(Milan Kundera - paraphrased by Jeffrey Rosen)*

- **2001.** Privacy protects us from being misrepresented and judged out of context...in a world in which information can easily be confused with knowledge. *(Jeffrey Rosen)*

- **2015.** We believe that people have a fundamental right to privacy. The American people demand it, the constitution demands it, morality demands it. *(Tim Cook)*
Some Parting Thoughts

- After 20 years working on privacy I still don’t have THE answer (and neither does anyone else)
- The value and definition of privacy continue to evolve; push/pull driven by technology and data
- Constant tension between stated desire for privacy versus willingness to give up personal info in return for something
- Fear of “privacy fatigue” and privacy becoming a “luxury good”

(Some) Resources

The Privacy Officer

- **Goal:** Balance privacy with business enablement
- **Role**
  - Collaboratively coordinate and manage risks and impacts the collection, use and sharing of personal information (information privacy), and the privacy risks and impacts related to freedom of intrusion (autonomy privacy).
  - Collaboratively coordinate and manage risks and impacts related to privacy laws, policies, and best practices
- **History**
  - The job itself is relatively new (circa 1996 in U.S.) and was created to respond to concern over the use of personal information, including medical data, financial information, and consumer data.
  - Privacy officers are even newer in higher ed, and most institutions do not have a designated privacy role.
## (Some) Resources

- Center for Democracy & Technology ([cdt.org/](http://cdt.org/))
- Electronic Privacy Information Center ([epic.org/](http://epic.org/))
- International Association of Privacy Professionals ([iapp.org](http://iapp.org))
- Privacy Rights Clearinghouse ([privacyrights.org/](http://privacyrights.org/))
- StaySafeOnline ([staysafeonline.org/](http://staysafeonline.org/))
- Stop Think Connect ([stopthinkconnect.org/](http://stopthinkconnect.org/))
- Fair Information Privacy Principles ([nist.gov/nstic/NSTIC-FIPPs.pdf](http://nist.gov/nstic/NSTIC-FIPPs.pdf))