Privacy Explained?
&
Getting to know the CPO

Sol Bermann, University of Michigan
Susan Blair, University of Florida
Kent Wada, UCLA (in absentia)

Educause Security Professionals Conference
May 2015
Privacy Explained? 
(in 20 minutes or less)
Imagine a world suddenly devoid of doors. None in your home, on dressing

Big Data and the Underground Railroad

Industry and government say “collect everything.” History suggests this is a bad idea.

or, more recently, Jennifer Lawrence’s nude selfies, made your vulnerability to cyber snooping abundantly clear.

You need only read George Orwell’s “1984” or watch the film Report to understand how incompatible with a free increasingly, people are coming to understand how their online data might

Privacy And Security: Is It Really Dead?

I wrote a post called, Privacy Is Completely And Unnecessarily Dead. It went off the same way I started off asking the same question.

Snapchat offers false sense of privacy; hackers threaten to leaking nude photos

Terms and Conditions, they look at and approach privacy, does privacy even matter anymore?”

Not on a Social Network? You’ve Still Got a Privacy Problem

Americans Say They Want Privacy, but Act as if They Don’t
Privacy Defined

Privacy v. Security

- Privacy is keeping something from someone, security is having the confidence that things are going to be ok
- Privacy deals more on the side of personal issues while security deals with financial issues
- Privacy like more like...personal info. Security...means a firewall, a secure site, and a good filter on your computer.

*(Pew Research 2014)
Privacy Defined (the “experts”)?

• 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, 1890)

• 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, 1967)

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

• 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, 2010)

• Building and maintaining an enduring, intimate relationship is a process of privacy regulation (Irwin Altman, 2014)
In American society today records mediate relationships between individuals and organizations and thus affect an individual more easily, more broadly, and often more unfairly...in an information-dependent society. (U. S. Privacy Study Commission, 1977)

Privacy’s Value

<table>
<thead>
<tr>
<th>Civil Liberties</th>
<th>Freedom of thought and speech</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Freedom of social and political activities</td>
</tr>
<tr>
<td></td>
<td>Limits authority</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Individual Liberties</th>
<th>Promotes individuality and respect for individuals</th>
</tr>
</thead>
<tbody>
<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>Not having to explain or justify oneself</td>
</tr>
</tbody>
</table>

<p>| Compliance                                          | FERPA, HIPAA, GLBA, COPPA, etc...                 |</p>
<table>
<thead>
<tr>
<th>Then</th>
<th>Now</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cameras</td>
<td>What doesn’t have a camera?!</td>
</tr>
<tr>
<td>News (periodic) - print, radio, TV</td>
<td>News (pervasive) - Social media</td>
</tr>
<tr>
<td>Phones</td>
<td>Smart phones, tablets</td>
</tr>
<tr>
<td>You &amp; your home</td>
<td>Google streetview, geo-location (satellite, cars, mobile devices), data-mining, apps</td>
</tr>
<tr>
<td>Disconnected devices</td>
<td>Internet of things: wearables, smart phones, smoke detectors, 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</td>
</tr>
<tr>
<td>Government surveillance - telephone</td>
<td>Government surveillance - NSA internet tapping, location tracking, facial recognition, pervasive data collection</td>
</tr>
<tr>
<td>wiretaps, tails</td>
<td></td>
</tr>
</tbody>
</table>
“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.”

61% would like to do more to protect their privacy.  
(Pew Research 2013 & 2014)

“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 (2014/01/19)
Privacy Issues in Higher Ed

- FERPA
- Common Rule (Human subject research)
- HIPAA
- GLBA
- Red Flags
- International privacy laws
- Privacy policies and notices
- SSNs/Identity Theft
- Google Apps for Education (and other external service providers)
- Big Data (ex: learning analytics)
- Social media
- and more...
Fun Fact!

Did you know that security is one of the cornerstones of the Fair Information Practice Principles (FIPPs)?

The Fair Information Practice Principles

To truly enhance privacy in the conduct of online transactions, Fair Information Practice Principles (FIPPs) must be universally and consistently adopted and applied in the Identity Ecosystem. FIPPs are the widely accepted framework of defining principles to be used in the evaluation and consideration of systems, processes, or programs that affect individual privacy.1

In brief, the Fair Information Practice Principles are:

- **Transparency**: Organizations should be transparent and notify individuals regarding collection, use, dissemination, and maintenance of personally identifiable information (PII).
- **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.
- **Security**: Organizations should protect PII (in all media) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.
- **Accountability and Auditing**: Organizations should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and auditing the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.
Privacy & Security Interplay

- Privacy is the policy and practices that describe how personal information is collected, used, and shared.
- Information security focuses on the technical controls that protect the data and systems on which it resides.

Privacy vs. Information Security

**Privacy: Focuses on individual’s ability to control PII**
- Identifying uses and users of PII
- Seeking agreement to use PII
- Limiting PII collection
- Limiting use of PII to identified purposes
- Being open, honest, and respectful
- Providing avenues for complaints
- Allowing access to PII to maintain accuracy and completeness

**Information Security: Focuses on mechanisms for protecting information and information systems**
- Ensuring availability of system
- Protecting both system and data from threats
  - Malicious code detection and prevention
  - Configuration and patch management
  - Intrusion detection and mitigation
- Physical protection

**Obvious differences**
- Accountability
- Integrity
- Aggregation
- Confidentiality
- Destruction

**Subtle differences (the intersection)**
Privacy & Security Interplay

- Another view*

*From the 2013 University of California privacy and information security initiative
Avoid this Interplay
● The Privacy Officer is primarily responsible for managing the risks and impacts related to privacy laws, policies, and best practices regarding the collection, use and sharing of personal information (information privacy); also manages privacy risks and impacts related to freedom of intrusion (autonomy privacy)

● The position 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 ([https://cdt.org/](https://cdt.org/))
- Electronic Privacy Information Center ([http://epic.org/](http://epic.org/))
- StaySafeOnline ([http://www.staysafeonline.org/](http://www.staysafeonline.org/))
- Stop Think Connect ([http://www.stopthinkconnect.org/](http://www.stopthinkconnect.org/))
How would you react if shopkeepers asked for the same permissions as apps?

https://youtu.be/xYZtHIPktQg