Privacy 2020
Where Have We Been and What’s Next?

Amelia Vance, Senior Counsel and Director of Youth & Education Privacy, Future of Privacy Forum

Is Privacy Dead?
New technologies contribute to privacy tensions

A Summary of Privacy (compiled from Soeme 2006)

<table>
<thead>
<tr>
<th>Domain</th>
<th>Privacy breach</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information</td>
<td>Surveillance</td>
<td>Watching, listening to, or recording of an individual’s activities</td>
</tr>
<tr>
<td>Collection</td>
<td>Interrogation</td>
<td>Various forms of questioning or probing for information</td>
</tr>
<tr>
<td>Processing</td>
<td>Aggregation</td>
<td>The combination of various pieces of data about a person</td>
</tr>
<tr>
<td></td>
<td>Identification</td>
<td>Linking information to particular individuals</td>
</tr>
<tr>
<td></td>
<td>Insecurity</td>
<td>Carelessness in protecting stored information from leaks and improper access</td>
</tr>
<tr>
<td></td>
<td>Secondary Use</td>
<td>Use of information collected for one purpose for a different purpose without the data subject’s consent</td>
</tr>
<tr>
<td></td>
<td>Exclusion</td>
<td>Failure to allow the data subject to know about the data that others have about her and participate in its handling and use, including being harmed from being able to access and correct errors</td>
</tr>
<tr>
<td>Information</td>
<td>Breach of Confidentiality</td>
<td>Breaking a promise to keep a person’s information confidential</td>
</tr>
<tr>
<td>Dissemination</td>
<td>Disclosure</td>
<td>Revelation of information about a person that impacts the way others judge her character</td>
</tr>
<tr>
<td></td>
<td>Exposure</td>
<td>Revealing another’s reality, grief, or bodily functions</td>
</tr>
<tr>
<td></td>
<td>Increased Accessibility</td>
<td>Amplifying the accessibility of information</td>
</tr>
<tr>
<td></td>
<td>Electrical</td>
<td>Threat to disclose personal information</td>
</tr>
<tr>
<td></td>
<td>Appropriation</td>
<td>The use of the data subject’s identity to serve the aims and interests of another</td>
</tr>
<tr>
<td></td>
<td>Distortion</td>
<td>Dissemination of false or misleading information about individuals</td>
</tr>
<tr>
<td>Invasion</td>
<td>Invasion</td>
<td>Invasive acts that disturb one’s tranquility or solitude</td>
</tr>
<tr>
<td>Decisional Interference</td>
<td>Decisional Interference</td>
<td>Ingression into the data subject’s decisions regarding her private affairs</td>
</tr>
</tbody>
</table>
It’s Not Really About Privacy

“Privacy was once misconstrued as being about hiding and secrecy. Now it’s understood to be something much more pressing: power dynamics between the individual, the state and the market. [Data protection] must seek to mitigate the inherent power imbalances between people — and those that collect, process and profit off their data.”

—Frederike Kaltheuner

Let’s Zoom Out...
In the past 10 years...

This is the decade that computers became the boss of you.
Tech Can Contribute to Privacy

To the 53 people who’ve watched A Christmas Prince every day for the past 18 days: Who hurt you?

6:52 PM - 10 Dec 2017

110,348 Retweets 442,580 Likes
Netflix’s ‘creepy’ tweet reminds us all how closely it’s watching us

So how did we get here?
Tech is being used to make big decisions, with no respect for context

The Secretive Company That Might End Privacy as We Know It

A little-known start-up helps law enforcement match photos of unknown people to their online images — and "might lead to a dystopian future or something," a belier says.

"...a tool that could end your ability to walk down the street anonymously, and provided it to hundreds of law enforcement agencies, ranging from local cops in Florida to the F.B.I. and the Department of Homeland Security..."
Uses Beyond Original Intent

Big Data & Found Data

- Transparency
- Individual Control
- Data Quality & Integrity
- Purpose Specification
- Use Limitation
- Data Minimization
- Security
- Accountability

New data sets and corporate research challenge Fair Information Practice Principles (FIPPS) and ethical research principles.

Breaches and Bad Actors

Adultery site Ashley Madison hacked, user data leaked

Data of 143 million Americans exposed in hack of credit reporting agency Equifax

Dozens of Norfolk students' private health information posted online by school system

'Dark Overlord' Hackers Text Death Threats to Students, Then Dump Voicemails From Victims
...Including Bad Actors Using Tech in Ways Never Intended

How might the tech my school has adopted be used to harm me?
How might the tech my school has adopted be used to harm me?

Colleges are turning student surveillance machines, tracking hundreds of thousands

Not Sure If They’re Invading My Privacy or Just Really Interested in Me

by Joseph Ekelund and Ben Shlifer

An analysis of 101 ECAK student and faculty data reveals that neither faculty nor students have a strong understanding of how their institutions use their personal data. Faculty have less confidence in their institutions’ abilities to safeguard private data than students do.

Campaign Calls for Banning Facial Recognition on College Campuses

How Privacy Has Traditionally Been Regulated
Privacy Safeguards in Law, Code, and Norms

- Broad legal protections against unfair or deceptive use of data
- Specific laws provide heightened protection for sensitive information (e.g. health, financial, kids)
- Technical measures reduce risk of unauthorized access (e.g. encryption, hashing, anti-scraping policies)
- Social norms constrain businesses and individuals who might otherwise use data in unexpected ways (aka “don’t be creepy”)

Looking Forward
Anatomy of a Privacy Law

by Daniel E. Solove

Scope and Applicability
- Scope of applicability?
- Sectors?
- Jurisdiction?
- Application?
- Exclusions?

Definition of Personal Data
- What is personal data?
- Examples?
- Sensitivity?

Processing of Personal Data
- Nature of processing?
- Purpose(s)?
- Lawfulness?
- Proportionality?
- Minimisation?

Data Subject Rights
- Right to access?
- Right to erasure?
- Right to rectification?
- Right to restrict processing?

Transfer of Data
- Cross-border transfer?
- Adequacy?
- Standard contractual clauses?

Consent
- Definition?
- Validity?
- Revoke consent?

Responsibilities
- Data controller?
- Data processor?
- Joint controller?

Enforcement
- Independent enforcement authority?
- Penalties?
- Compliance tools?

Compliance with Law
- Compliance?
- Security?
- Data protection impact assessment?

Adaptation of this tool for educational purposes is encouraged.
Technological Changes and Platform Incentives are a More Effective Determinant of Privacy than Law

Jules Polonetsky @JulesPolonetsky
Privacy2020 Prediction #1: Browser and OS changes will do more in 2020 to limit tracking than GDPR, CCPA or any other legislation.
5:30 AM - 27 Nov 2018 from Washington, DC

Innovations: Privacy Risks
- Biometric scanning
- Real-world evidence, social credit, and reputation scoring
- Internet of bodies
- Automation and robotics
- Location services and proximity tracking
- Smart communities, including educational agencies and institutions
- Quantum computing
- AR/VR (spatial computing)
Reminder: Tech Can Contribute to Privacy

Innovations: Privacy Protective

- Advances in deidentification and cryptography
- Localization of processing (device-level processing or machine learning, identity management)
- Advance in AI and machine learning (small data, synthetic data sets, etc)
Your Role
Basic Privacy Principles

- Transparency
- Control
- Purpose Specification
- Data Minimization
- Respect for Context
- Accuracy
- Security
- Accountability

Fair Information Practice Principles (FIPPs)

<table>
<thead>
<tr>
<th>Principle</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Transparency</strong></td>
<td>The entity should be transparent and provide notice to the individual regarding the collection, nature, dissemination, and maintenance of personally identifiable information (PII).</td>
</tr>
<tr>
<td><strong>Individual Participation</strong></td>
<td>The entity should ensure the individual is in the process of using PI and, to the extent practicable, seek the individual’s consent before the collection, use, disclosure, or maintenance of PI. The entity should also provide mechanisms for appropriate access, correction, and deletion regarding the entity’s uses of PI.</td>
</tr>
<tr>
<td><strong>Purpose Specification</strong></td>
<td>The entity should specifically articulate the purpose and scope of the collection, use, disclosure, or maintenance of PI. The entity should not use PI for any purpose unrelated to the stated purpose.</td>
</tr>
<tr>
<td><strong>Data Minimization</strong></td>
<td>The entity should only collect PI that is directly relevant and necessary to accomplish the specified purpose and only retain PI for as long as it is necessary to accomplish the specified purpose.</td>
</tr>
<tr>
<td><strong>Use Limitation</strong></td>
<td>The entity should use PI only for the purposes specified in the notice. Sharing PI outside the entity should be for a purpose consistent with the purpose for which the PI was collected.</td>
</tr>
<tr>
<td><strong>Data Quality and Integrity</strong></td>
<td>The entity should ensure PI is accurate, complete, and up-to-date.</td>
</tr>
<tr>
<td><strong>Security</strong></td>
<td>The entity should protect PI from risks such as unauthorized access or use, destruction, loss, alteration, or disclosure of PI.</td>
</tr>
<tr>
<td><strong>Accountability and Auditing</strong></td>
<td>The entity should be accountable for complying with these principles, providing training to all employees and contractors who process PI, and auditing the actual use of PI to ensure the entity is following all applicable privacy protection requirements.</td>
</tr>
</tbody>
</table>

Notice: Individuals are informed that data are being generated and the purpose to which the data will be put.

Choice: Individuals have the choice to opt-in or opt-out as to whether and how their data will be used or disclosed.

Consent: Data are only generated and disclosed with the consent of individuals.

Security: Data are protected from loss, misuse, unauthorized access, disclosure, alteration and destruction.

Integrity: Data are reliable, accurate, complete, and current.

Access: Individuals can access, check and verify data about themselves.

Accountability: The data holder is accountable for ensuring the above principles and has mechanisms in place to assure compliance.
Privacy norms are different in every community, continually change, and are contextual

Essential Questions
- What questions are you trying to answer or what problem are you trying to solve?
- Where’s your community’s “creepy line”?
- What are the privacy risks posed by how you are collecting, using, storing, or sharing data? The key benefits?
- What governance structures, policies, and procedures do you have in place?
- How can you be proactive about public communication and engagement around privacy?
Making Privacy Important

- Make it personal: what do you keep private?
- Make it what they care about - whether their personal politics and beliefs or your institution’s reputation, legal liability, and ability to be a leader on this issue
- This isn’t just “privacy” - it’s your whole life, online and offline, everywhere you are, everything you do, everything you think.

Again - It’s Not Really About Privacy

“Privacy was once misconstrued as being about hiding and secrecy. Now it’s understood to be something much more pressing: power dynamics between the individual, the state and the market. [Data protection] must seek to mitigate the inherent power imbalances between people — and those that collect, process and profit off their data.”

— Frederike Kaltheuner
The Goal: Creating a Culture of Privacy

Questions?

- advance@fpf.org
- www.fpf.org
- facebook.com/futureofprivacy
- @futureofprivacy