Privacy Threats

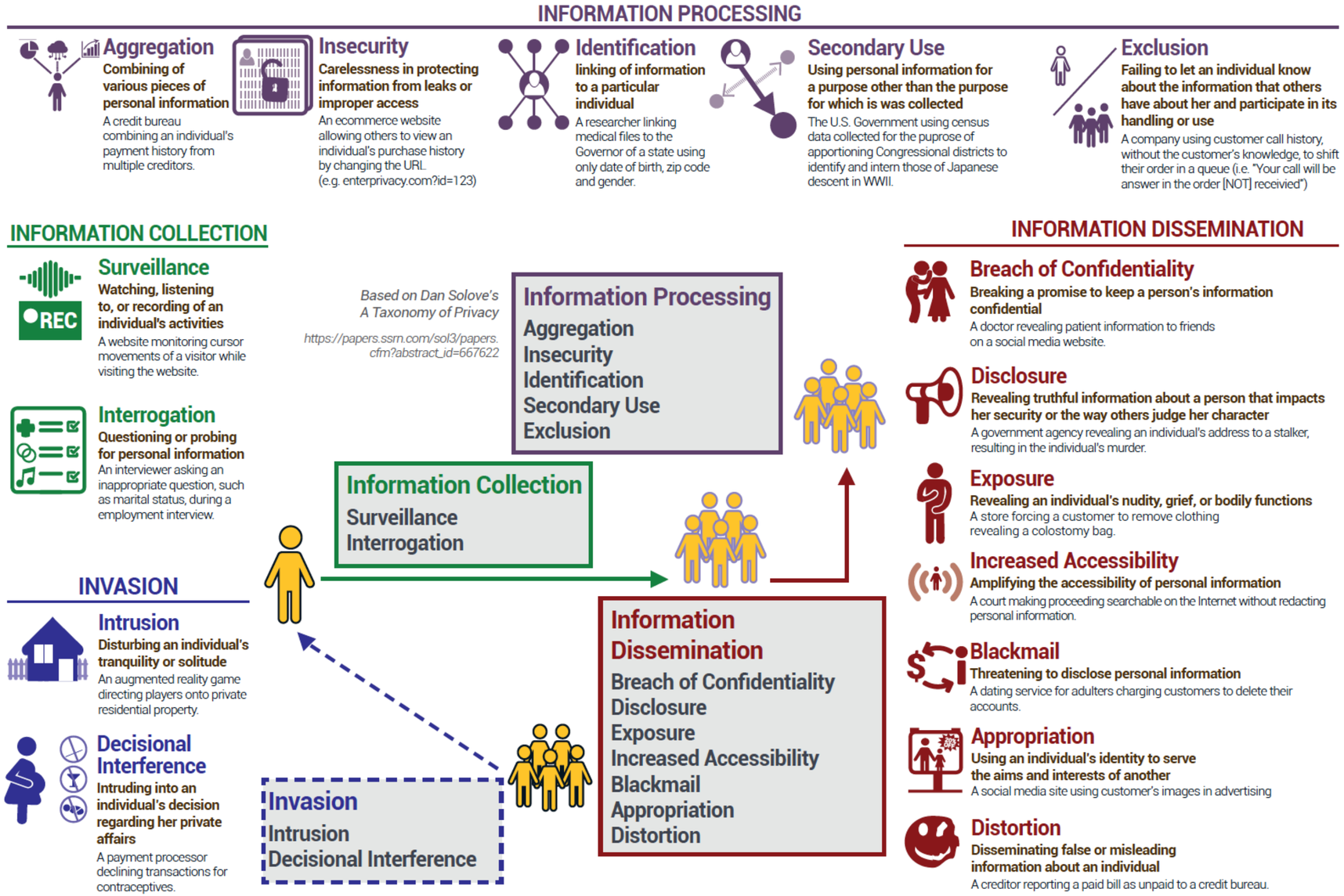
Lecture Outline

- Privacy threats
- Privacy enhancing solutions (PETs)

Learning Outcomes

- At the end of this lecture you should be able to:
  - Provide examples of privacy threats
  - Link privacy enhancing technologies to privacy threats

Solove's Privacy Taxonomy



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.

Information Collection: Surveillance

- *"Smart meters are presented as an environmental and power-saving initiative. But it's a highly surveillant model. It can tell how many showers you have had, when you are cooking, when you are in and out of the home."*

- *"We take energy consumption data from smart meters and sensors. We analyse it and build a highly personalised profile for each and every utility customer"* (0nzo, British Analytics Company).

Information Collection: Surveillance

BRIAN BARRETT SECURITY 02.07.17 08:03 PM

HOW TO STOP YOUR SMART TV FROM SPYING ON YOU

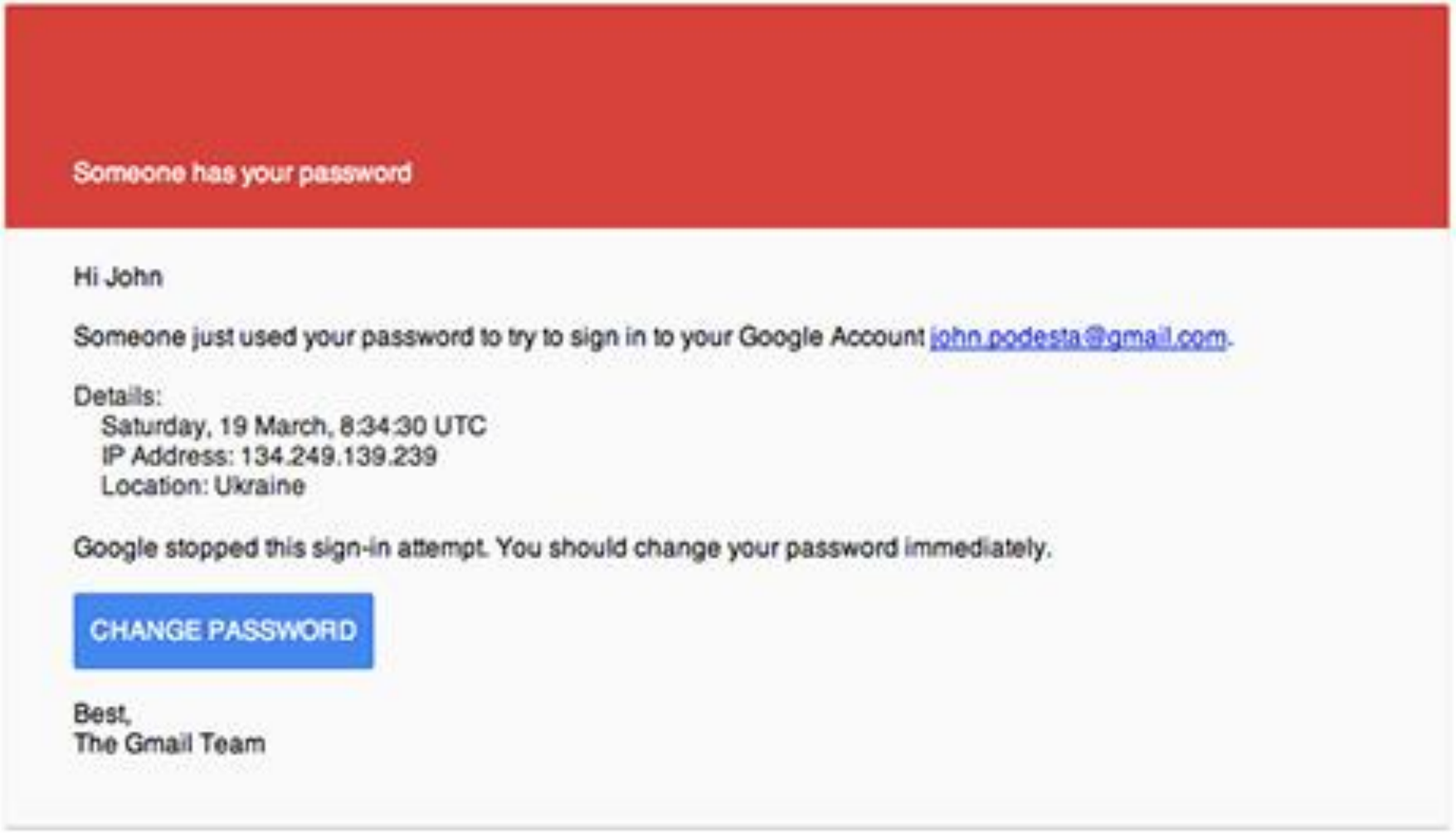
THIS WEEK, VIZIO, which makes popular, high-quality, affordable TV sets, agreed to pay a $2.2 million fine to the FTC. As it turns out, those same TVs were also busily tracking what their owners were watching, and shuttling that data back to the company's servers, where it would be sold to eager advertisers.

Information Collection: Surveillance

Angry Birds and 'leaky' phone apps targeted by NSA and GCHQ for user data

- US and UK spy agencies piggyback on commercial data
- Details can include age, location and sexual orientation
- Documents also reveal targeted tools against individual phones

Information Collection: Probing



Someone has your password

Hi John

Someone just used your password to try to sign in to your Google Account john.podesta@gmail.com.

Details:
Saturday, 19 March, 8:34:30 UTC
IP Address: 134.249.139.239
Location: Ukraine

Google stopped this sign-in attempt. You should change your password immediately.

CHANGE PASSWORD

Best,
The Gmail Team

Information Processing

- *Aggregation*
  - involves the combination of various pieces of data about a person.
- *Identification*
  - 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

Information Processing: Aggregation

How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did

Kashmir Hill, FORBES STAFF
Welcome to The Not-So Private Parts where technology & privacy collide
FULL BIO

Every time you go shopping, you share intimate details about your consumption patterns with retailers. And many of those retailers are studying those details to figure out what you like, what you need, and which coupons are most likely to make you happy. Target TGT +2.2%, for example, has figured out how to

Information Processing: Identification

On the Web's Cutting Edge, Anonymity in Name Only

Posted on August 3, 2010 by juliaangwin — No Comments ↓

The Wall Street Journal, Page One

You may not know a company called [x+1] Inc., but it may well know a lot about you.

From a single click on a web site, [x+1] correctly identified Carrie Isaac as a young Colorado Springs parent who lives on about $50,000 a year, shops at Wal-Mart and rents kids' videos. The company deduced that Paul Boulifard, a Nashville architect, is childless, likes to travel and buys used cars. And [x+1] determined that Thomas Burney, a Colorado building contractor, is a skier with a college degree and looks like he has good credit.

The company didn't get every detail correct. But its ability to make snap assessments of individuals is accurate enough that Capital One Financial Corp. uses [x+1]'s calculations to instantly decide which credit cards to show first-time visitors to its website.

Information Processing: Secondary Use

Information Dissemination

- *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 Processing: Breach to Confidentiality

Equifax finds more victims of 2017 breach

1 March 2018

Share

US politicians have criticised Equifax, saying that it "botched" its earlier response to the breach

The massive data breach suffered by credit-rating company Equifax hit more people than previously thought, the company has reported.

Information Dissemination: Exposure

Massive Leak of Celebrity Nude Photos Calls Cloud Security Into Question

PREVIOUS CONTRIBUTORS

SEP 1, 2014 | VULNERABILITY MANAGEMENT

Information Dissemination: Appropriation

Identity fraud up by 57% as thieves 'hunt' on social media

5 July 2016 | UK

Share

The BBC's Angus Crawford went on the trail of identity fraudsters last year

Information Dissemination: Blackmail

Invasions

- *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

Invasions: Intrusion

Social networking sites fuelling stalking, report warns

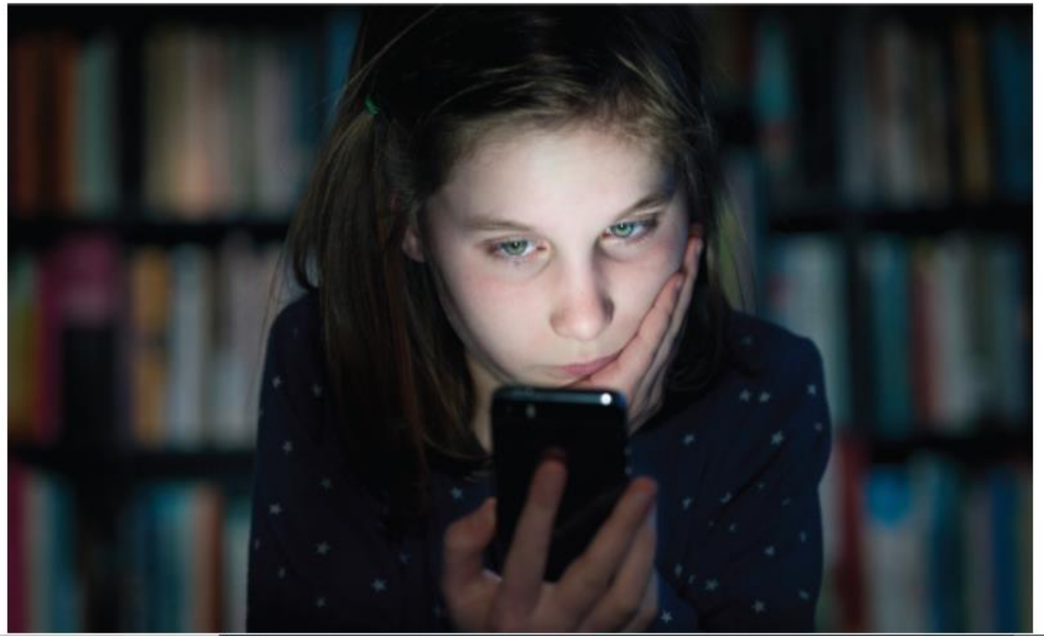
Smartphones and social networking sites are making it much easier for stalkers to target victims, say charities

Invasions: Intrusion

A Majority of Teens Have Experienced Some Form of Cyberbullying

59% of U.S. teens have been bullied or harassed online, and a similar share says it's a major problem for people their age. At the same time, teens mostly think teachers, social media companies and politicians are failing at addressing this issue.

BY MONICA ANDERSON



Privacy Enhancing Technologies (PETS)

Privacy Enhancing Technologies (PETS)

- Tools, mechanism or architectures that aim to mitigate privacy concerns
  - While allowing users to enjoy the benefits of modern technologies
- PETS can be applied to communications or to existing databases
- PETS can be deployed either by individual users or by organizations

Data Protection Technologies

- Help to design information and communication systems and services in a way that minimizes the collection and use of personal data and facilitate compliance with data protection rules
- They should result in making breaches of certain data protection rules more difficult and/or helping to detect them
- Examples
  - Encryption of data at rest and in transmission
  - Authentication and Authorization of employees handling personal data
  - Secure logging of data accesses and processing activities for audit purposes
  - Secure deletion of data (right to be forgotten)
  - Purpose-based access control

User Awareness Technologies

- Set of technologies that allow a user to choose if, when and under what circumstances personal information is disclosed
- They help users make informed choices about privacy protection
- Examples:
  - Privacy friendly defaults
  - Usable privacy settings, contextual feedback, dashboard for privacy management
  - Usable interfaces for the exercise of subject access rights
  - Clear, concise and understandable privacy policies
  - Privacy nudges

Privacy Bird

Shane Zachary Cranor's Home Page - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Favorites Media History Print

Address http://shane.cranor.org/

Shane Zachary Cranor

Born May 4, 2001, 7:25 am, 7 pounds, 13 oz., 21 incl

Photo Album | Latest Photos | 2001 Favorite Phot
Favorite Photos

Shane's Photo Album

- Shane's First Year

Shane's Latest Photos

Shane attended Mom's Chatham Community Band Concert, but he was so bored
The next day Shane helped Dad change a lightbulb -- climbing a ladder couldn't

Policy Summary

Shane Cranor's Home Page Privacy Practices

Privacy Policy Check

Shane Cranor's Home Page's privacy policy *matches your preferences.*

Privacy Policy Summary

This site has the following statements in its policy:

- Site Statement 1

Site Statement 1

Types of Information Collected:

- HTTP protocol information
- Click-stream information

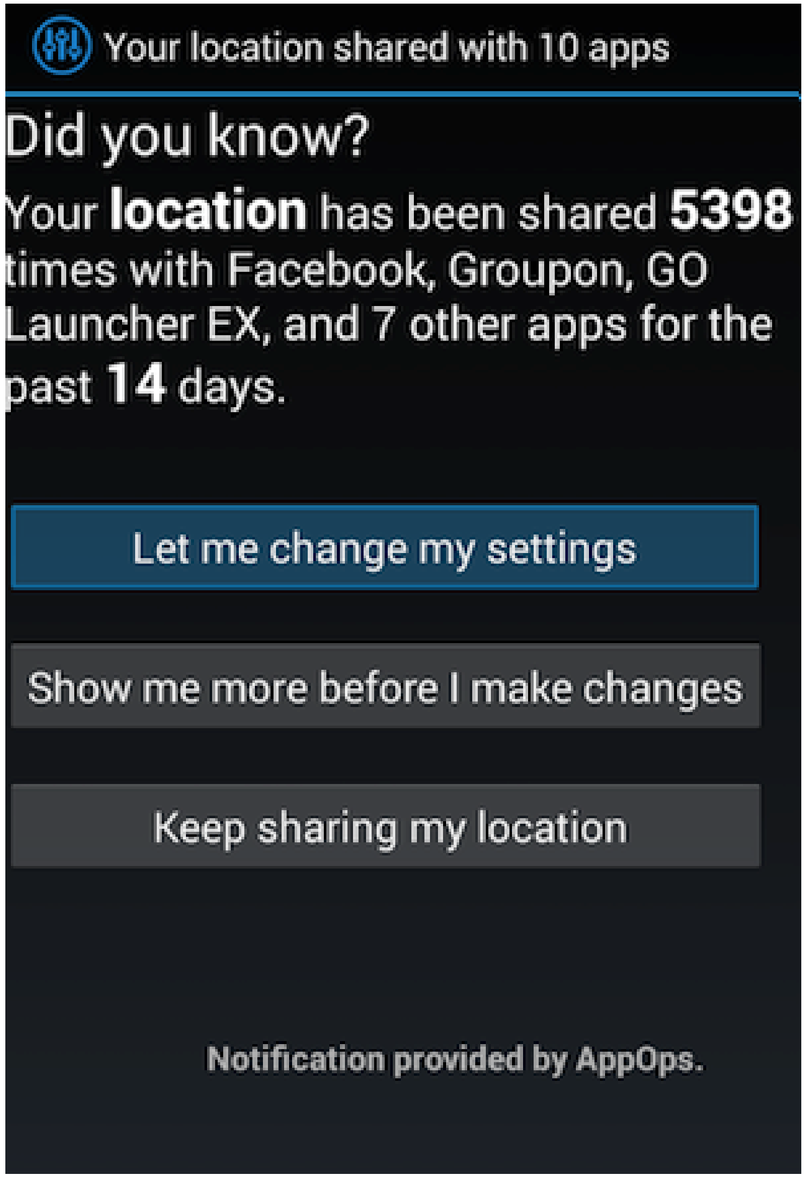
How your information will be used:

- Research and development
- To complete the activity for which the data was provided
- Web site and system administration

Who will use your information:

- This web site and its agents

Privacy Nudges



Anonimity Technologies

- Ensure Anonimity
- Examples
  - Database anonymity: k-anonymity, l-diversity, t-closeness
  - Anonymous communications: Mixnets, Onion routing, Tor
  - Anonymous credentials: Idemix (IBM)

Other Privacy Enhancing Technologies

- Private remote storage
  - PrivateStorage
- Searchable Encryption
- Privacy preserving computations
  - Homomorphic encryption
  - Secure multiparty computation

Summary

- Defining privacy is difficult
- Privacy Technologies
  - Data protection technologies
  - User awareness technologies
  - Anonymity technologies

Resources

- Daniel J. Solove. A Taxonomy of Privacy. Available at: https://www.law.upenn.edu/journals/lawreview/articles/volume154/issue3/Solove154U.Pa.L.Rev.477(2006).pdf
- Enisa report on Privacy and Data Protection by Design – from policy to engineering 2014