Lecture 27: Privacy

CS 5430
Confidentiality
Integrity
Availability
Privacy

*Privacy* concerns information about individuals (people, organizations, etc.)

- Often construed as legal right
- *Privacy* is not a synonym for confidentiality or for secrecy
What is Privacy?
What is a privacy violation?

- Police read papers stored in your home
- Police read papers you threw in the trash
- Police read your medical records
- Your parents read your medical records
- Gannett uses your medical records in a research study
- Police read your texts/Facebook messages
- Police read your emails
- Google employee reads your emails
- Google uses your emails to target personalized ads
- Someone tracks your location for months (using phone)
Privacy in American Law
Contextual Integrity

- defines privacy relative to appropriate context
- considers information type, time, location, purpose, principals involved (subject, sender, receiver)
- dependent on social norms
- norms can change over time
General Guidelines

The FTC's Fair Information Practice Principals (FIPPs) are the most broadly recognized guidelines for handling private data in information systems

- Seek consent
- Minimize data use
- Limit storage
- Avoid linking
Deanonymization

[Diagram showing Venn diagram with three circles: Zip Code, Gender, Date of Birth. The intersection is labeled as You.]
Deanonymization
Deanonymization

NETFLIX
## k-Anonymity

<table>
<thead>
<tr>
<th>Name</th>
<th>Gender</th>
<th>Year</th>
<th>Grade</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alice</td>
<td>F</td>
<td>2018</td>
<td>95</td>
</tr>
<tr>
<td>Bob</td>
<td>M</td>
<td>2018</td>
<td>80</td>
</tr>
<tr>
<td>Charlie</td>
<td>M</td>
<td>2018</td>
<td>95</td>
</tr>
<tr>
<td>David</td>
<td>M</td>
<td>2018</td>
<td>60</td>
</tr>
<tr>
<td>Edward</td>
<td>M</td>
<td>2019</td>
<td>80</td>
</tr>
<tr>
<td>Flora</td>
<td>F</td>
<td>2019</td>
<td>99</td>
</tr>
<tr>
<td>Georgia</td>
<td>F</td>
<td>2019</td>
<td>60</td>
</tr>
</tbody>
</table>
Database Privacy

Offline Privacy

Online Privacy
Data Perturbation

<table>
<thead>
<tr>
<th>Group</th>
<th>ClassVar</th>
<th>OpVal</th>
<th>Recover</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Differential Privacy

- absolute privacy is impossible
- goal should be to limit how much information can be learned

A query $Q$ is $\epsilon$-differentially private if $\forall D, r \in D$,

$$\Pr[Q(D) = x] \leq e^{\epsilon} \cdot \Pr[Q(D - r) = x]$$
Differential Privacy

Key Idea: Changing a single user’s record does not significantly affect the result of any analysis or query.
DP in action...
Internet Privacy

"On the Internet, nobody knows you're a dog."
Internet Privacy

The Joy of Tech™

In the 1990’s

ON THE INTERNET, NOBODY KNOWS YOU’RE A DOG.

Now

OUR METADATA ANALYSIS INDICATES THAT HE IS DEFINITELY A BROWN LAB.

HE LIVES WITH A WHITE AND BLACK SPOTTED BEAGLE-MIX, AND I SUSPECT THEY ARE HUMPING.

© 2013 Geek Culture

joyoftech.com
Notice & Consent
Personal Tech

US Senate votes to let broadband ISPs sell your browser histories

Hear that? That's the sound of ringing tills, sorry, freedom

23 Mar 2017 at 19:23, Kieren McCarthy
Browser Tracking
### Browser Tracking

**Truth. It's more important now than ever.**

**The New York Times**
Thursday, March 23, 2017 | Video | 32°F | Hang Seng -0.09%

Support our mission in a new way.

When you buy any bag of dog or cat food, we give a meal to a pet in need.

---

<table>
<thead>
<tr>
<th>Name</th>
<th>Domain</th>
<th>Method</th>
<th>Schema</th>
<th>Status</th>
<th>Cacheable</th>
<th>Size</th>
<th>Transfer</th>
<th>Start Time</th>
<th>Latency</th>
<th>Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>blob:<a href="https://www.youtube.com/8a5f5e3-99f3-">https://www.youtube.com/8a5f5e3-99f3-</a>...</td>
<td>a1.nyt.com</td>
<td>GET</td>
<td>HTTPS</td>
<td>Yes</td>
<td>0 B</td>
<td>437.57 KB</td>
<td>311.1ms</td>
<td>19.79ms</td>
<td>149.2ms</td>
<td></td>
</tr>
<tr>
<td>tagx-simple.min.js</td>
<td>a248.e.akamai.net</td>
<td>GET</td>
<td>HTTPS</td>
<td>Yes</td>
<td>0 B</td>
<td>32.56 KB</td>
<td>7.60s</td>
<td>24.03ms</td>
<td>0.154ms</td>
<td></td>
</tr>
<tr>
<td>sharetools-mixin.js</td>
<td>ad.doubleclick.net</td>
<td>GET</td>
<td>HTTPS</td>
<td>No</td>
<td>42 B</td>
<td>559 B</td>
<td>18.93s</td>
<td>62.15ms</td>
<td>0.911ms</td>
<td></td>
</tr>
<tr>
<td>sharetools-config.js</td>
<td>ad.doubleclick.net</td>
<td>GET</td>
<td>HTTPS</td>
<td>No</td>
<td>42 B</td>
<td>559 B</td>
<td>17.20s</td>
<td>244.0ms</td>
<td>0.839ms</td>
<td></td>
</tr>
<tr>
<td>showall.js</td>
<td>ad.doubleclick.net</td>
<td>GET</td>
<td>HTTPS</td>
<td>No</td>
<td>42 B</td>
<td>559 B</td>
<td>5.23s</td>
<td>125.6ms</td>
<td>0.658ms</td>
<td></td>
</tr>
<tr>
<td>sharetools.js</td>
<td>ads.undertone.com</td>
<td>GET</td>
<td>HTTPS</td>
<td>No</td>
<td>7 B</td>
<td>129 B</td>
<td>9.68s</td>
<td>1.09s</td>
<td>0.248ms</td>
<td></td>
</tr>
<tr>
<td>fonts.css</td>
<td>ag.innovid.com</td>
<td>GET</td>
<td>HTTPS</td>
<td>No</td>
<td>43 B</td>
<td>288 B</td>
<td>9.69s</td>
<td>996.8ms</td>
<td>1.076ms</td>
<td></td>
</tr>
<tr>
<td>ad-view-manager.js</td>
<td>analytics.twitter.com</td>
<td>GET</td>
<td>HTTPS</td>
<td>No</td>
<td>—</td>
<td>604 B</td>
<td>7.17s</td>
<td>1.14s</td>
<td>0.425ms</td>
<td></td>
</tr>
<tr>
<td>1.6.0.js</td>
<td>beacon.krxd.net</td>
<td>GET</td>
<td>HTTPS</td>
<td>No</td>
<td>—</td>
<td>491 B</td>
<td>9.62s</td>
<td>2.13s</td>
<td>5.757ms</td>
<td></td>
</tr>
</tbody>
</table>
Beyond Cookies

Zombie Cookies

Browser Fingerprinting
Fingerprinting Works

Operating System

Browser

Settings

Time Zone

Language

Canvas
The result...

Your categories

Below you can review the interests and inferred demographics that Google has associated with your cookie. You can remove or edit these at any time.

Business & Industrial

Business & Industrial - Manufacturing

Computers & Electronics - Computer Hardware - Laptops & Notebooks - Tablet PCs

Computers & Electronics - Software - Multimedia Software - Photo & Video Software

Computers & Electronics - Software - Operating Systems - Mac OS

Internet & Telecom - Mobile & Wireless - Mobile Phones

Internet & Telecom - Mobile & Wireless - Mobile Phones - Smart Phones

Online Communities - Social Networks

Reference - General Reference - Time & Calendars

Science - Mathematics
Personalized Content

I used to fetch his newspaper... now I just forward articles I know he'll agree with.
Targeted Advertising

I think my Nest smoke alarm is going off. Google AdWords just pitched me a fire extinguisher and an offer for temporary housing.
Data Collection is Here to Stay…

“Remember when, on the Internet, nobody knew who you were?”