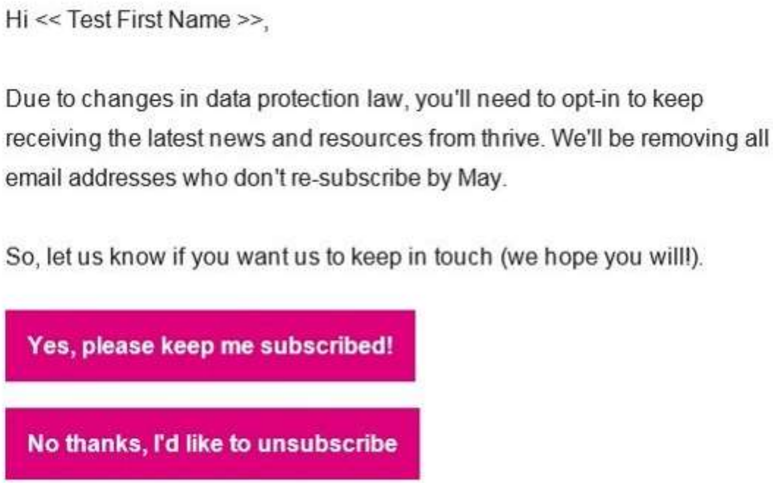
Privacy

Blase Ur, David Cash, Ben Zhao

UChicago CMSC 23200/33250

Privacy Is Dead

Privacy in 2018



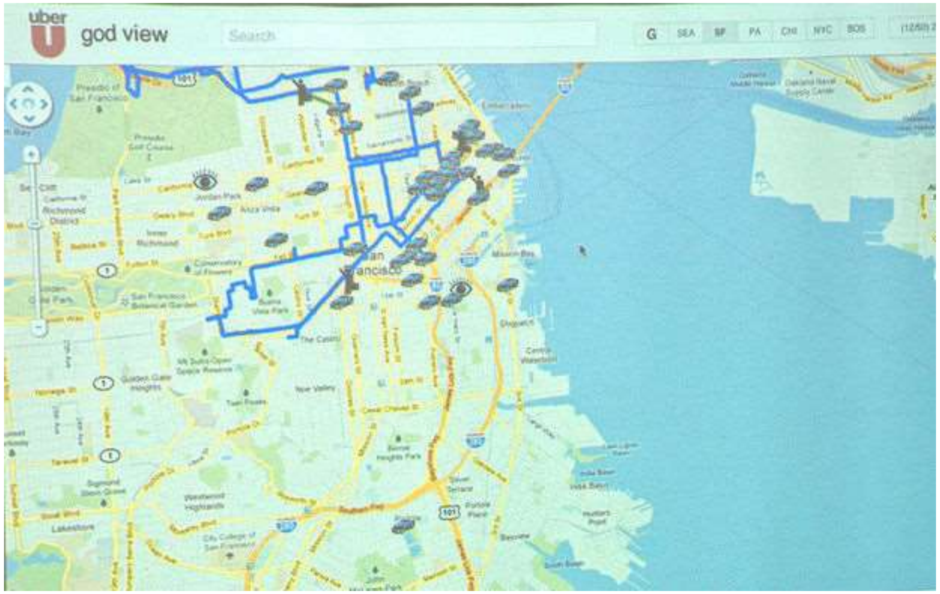
Hi << Test First Name >>,

Due to changes in data protection law, you'll need to opt-in to keep receiving the latest news and resources from thrive. We'll be removing all email addresses who don't re-subscribe by May.

So, let us know if you want us to keep in touch (we hope you will!).

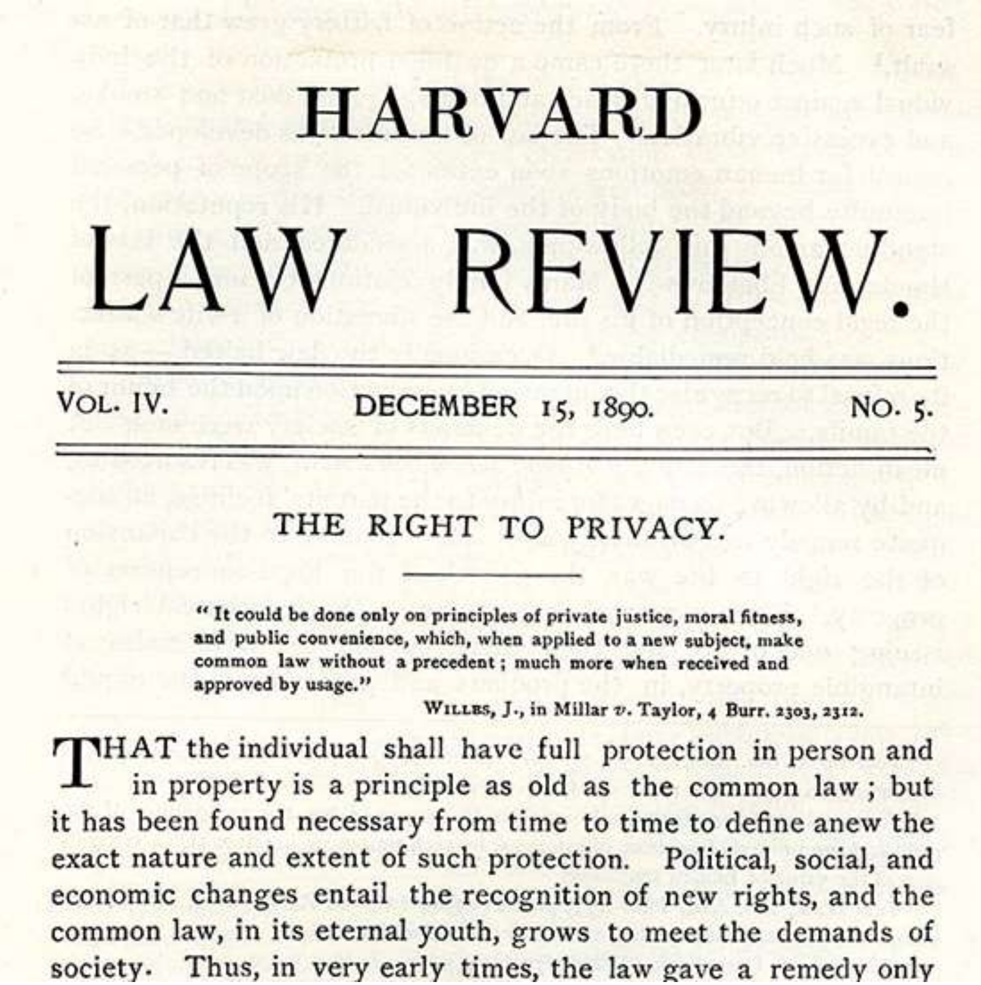
Yes, please keep me subscribed!
No thanks, I'd like to unsubscribe

Privacy in the Last Few Years



EQUIFAX

Warren and Brandeis (1890)



HARVARD

LAW REVIEW.

VOL. IV. DECEMBER 15, 1890. NO. 5.

THE RIGHT TO PRIVACY.

> "It could be done only on principles of private justice, moral fitness, and public convenience, which, when applied to a new subject, make common law without a precedent; much more when received and approved by usage."
>
> WILLES, J., in Millar *v.* Taylor, 4 Burr. 2303, 2312.

THAT the individual shall have full protection in person and in property is a principle as old as the common law; but it has been found necessary from time to time to define anew the exact nature and extent of such protection. Political, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the demands of society. Thus, in very early times, the law gave a remedy only

Warren and Brandeis's Argument

- Libel and slander are insufficient in considering only damage to reputation
- Considers property rights
- The right to prevent, rather than profit from, publication
- **"The right to be let alone"**
- Excludes topics of general interest

Privacy as Control / Secrecy (1967)

“Privacy is the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.”

“…each individual is continually engaged in a personal adjustment process in which he balances the desire for privacy with the desire for disclosure and communication….”

Alan Westin, Privacy and Freedom, 1967

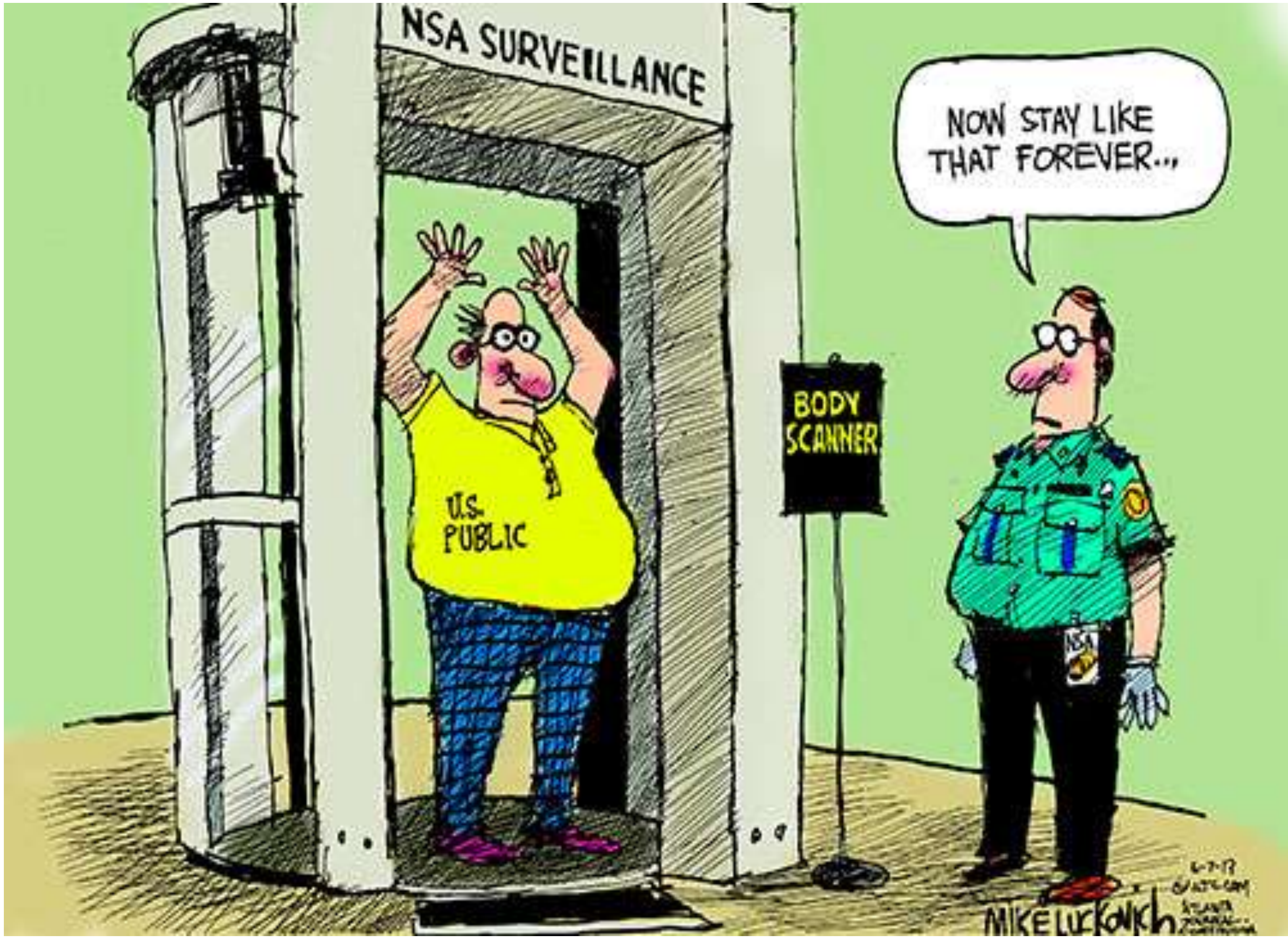
Privacy Regulation Theory (1975)

- Irwin Altman (social psychology)
  - Preceded by Altman and Taylor's Social Penetration Theory (1973) about intimacy in relationships
- Dialectic and dynamic process of boundary regulation
  - Continuous movement on a continuum
- Goal: optimum balance of privacy and social interaction

CPM Theory (1991)

- Sandra Petronio (communications)
  - Communication Privacy Management Theory
- Regulate boundaries based on perceived costs and benefits
  - Movement on a continuum
- Expect rule-based management
- Boundary turbulence related to clashing expectations

Purpose Matters **(?)**



Privacy as Contextual Integrity (2004)

- Helen Nissenbaum (philosophy)
- “Contextual integrity ties adequate protection for privacy to norms of specific contexts, demanding that information gathering and dissemination be appropriate to that context.”

Privacy as Contextual Integrity

- Appropriate flows of information
- Appropriate flows conform to contextual information norms
- Norms refer to the data subject, sender, recipient, information type, and transmission principle
- Conceptions of privacy evolve over time and are grounded in ethics

Dan Solove’s Pluralistic Conceptions

- Some data isn’t “sensitive,” but its collection and use impact privacy
  - Impact power relationships
  - Kafka-esque
- Solove’s privacy taxonomy
  - Information collection
  - Information processing
  - Information dissemination
  - Invasion

Issues of privacy

- Can conflict with free speech / security
- How do we quantify privacy harms?
- Can we measure chilling effects?
- How do we provide transparency?
- Distortion: false of misleading information
- Data mining → future activities?
- Oversight and accountability

Privacy laws around the world

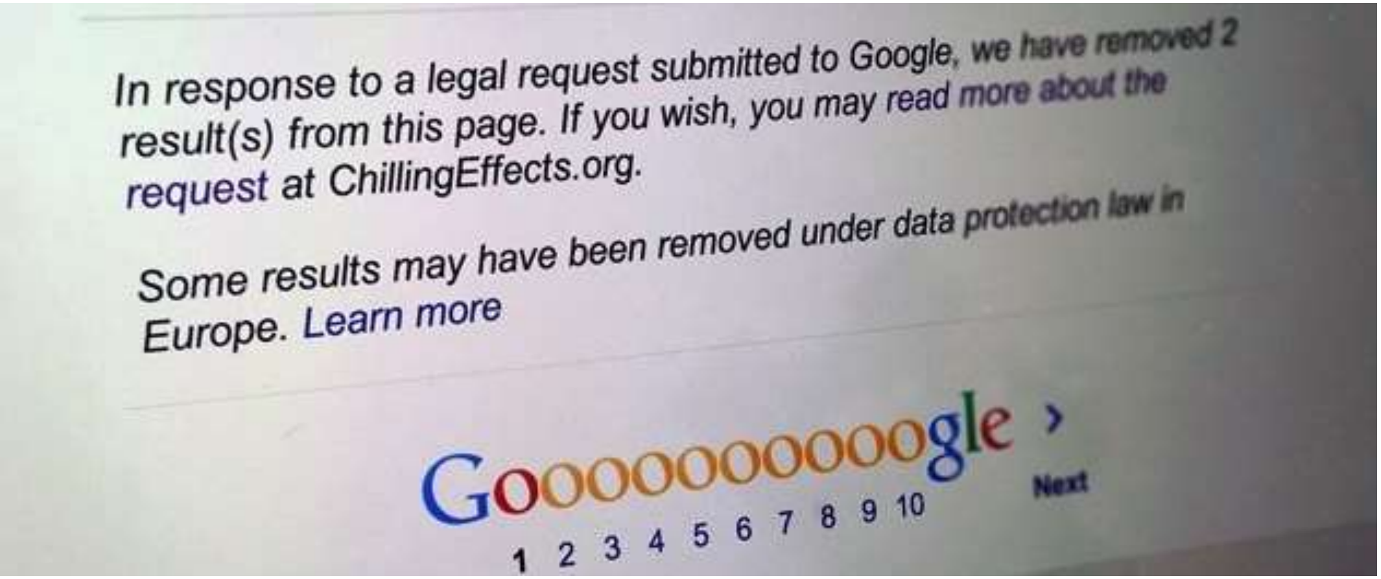
- US has sector-specific laws, minimal protections
  - No explicit constitutional right to privacy or general privacy law
  - Some privacy rights inferred from constitution
  - Narrow regulations for health, credit, education, videos, children, financial information
  - FTC investigates fraud & deceptive practices
  - FCC regulates telecommunications
  - Some state and local laws (California)

EU GDPR (2016/679)

- General Data Protection Regulation
- Disclose collection, automated decisions
- Data protection by design and default
- Right of access
- Right of erasure (right to be forgotten)
- Data breach notification within 72 hours
- Penalty: Up to 2%/4% of worldwide turnover

Right to be forgotten

- Should a person have the agency to cause items from the past to be removed?
- Who owns information?
- EU



In response to a legal request submitted to Google, we have removed 2 result(s) from this page. If you wish, you may read more about the request at ChillingEffects.org.

Some results may have been removed under data protection law in Europe. Learn more

Fair Information Practice Principles

- Notice / Awareness
- Choice / Consent
- Access / Participation
- Integrity / Security
- Enforcement / Redress

Privacy Is Hard

- AOL search keywords (2006)
  - 20 million searches from 650,000 “anonymous” users

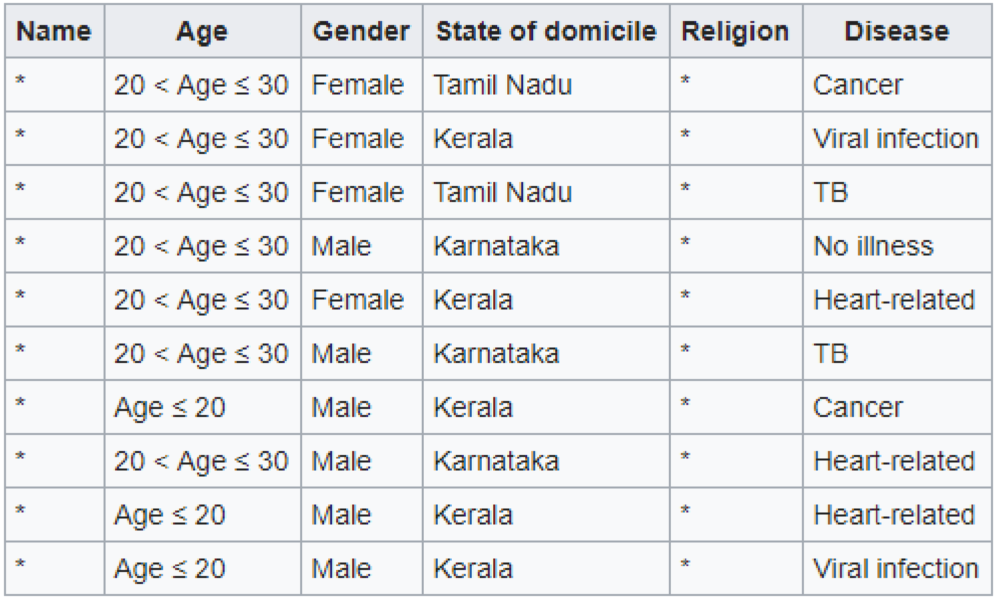
- Netflix Prize Dataset

NETFLIX

IMDb

k-Anonymity (1998)

- Latanya Sweeney / Pierangela Samarati
- Each person cannot be distinguished from k-1 other individuals in the database



Name	Age	Gender	State of domicile	Religion	Disease
*	20 < Age ≤ 30	Female	Tamil Nadu	*	Cancer
*	20 < Age ≤ 30	Female	Kerala	*	Viral infection
*	20 < Age ≤ 30	Female	Tamil Nadu	*	TB
*	20 < Age ≤ 30	Male	Karnataka	*	No illness
*	20 < Age ≤ 30	Female	Kerala	*	Heart-related
*	20 < Age ≤ 30	Male	Karnataka	*	TB
*	Age ≤ 20	Male	Kerala	*	Cancer
*	20 < Age ≤ 30	Male	Karnataka	*	Heart-related
*	Age ≤ 20	Male	Kerala	*	Heart-related
*	Age ≤ 20	Male	Kerala	*	Viral infection

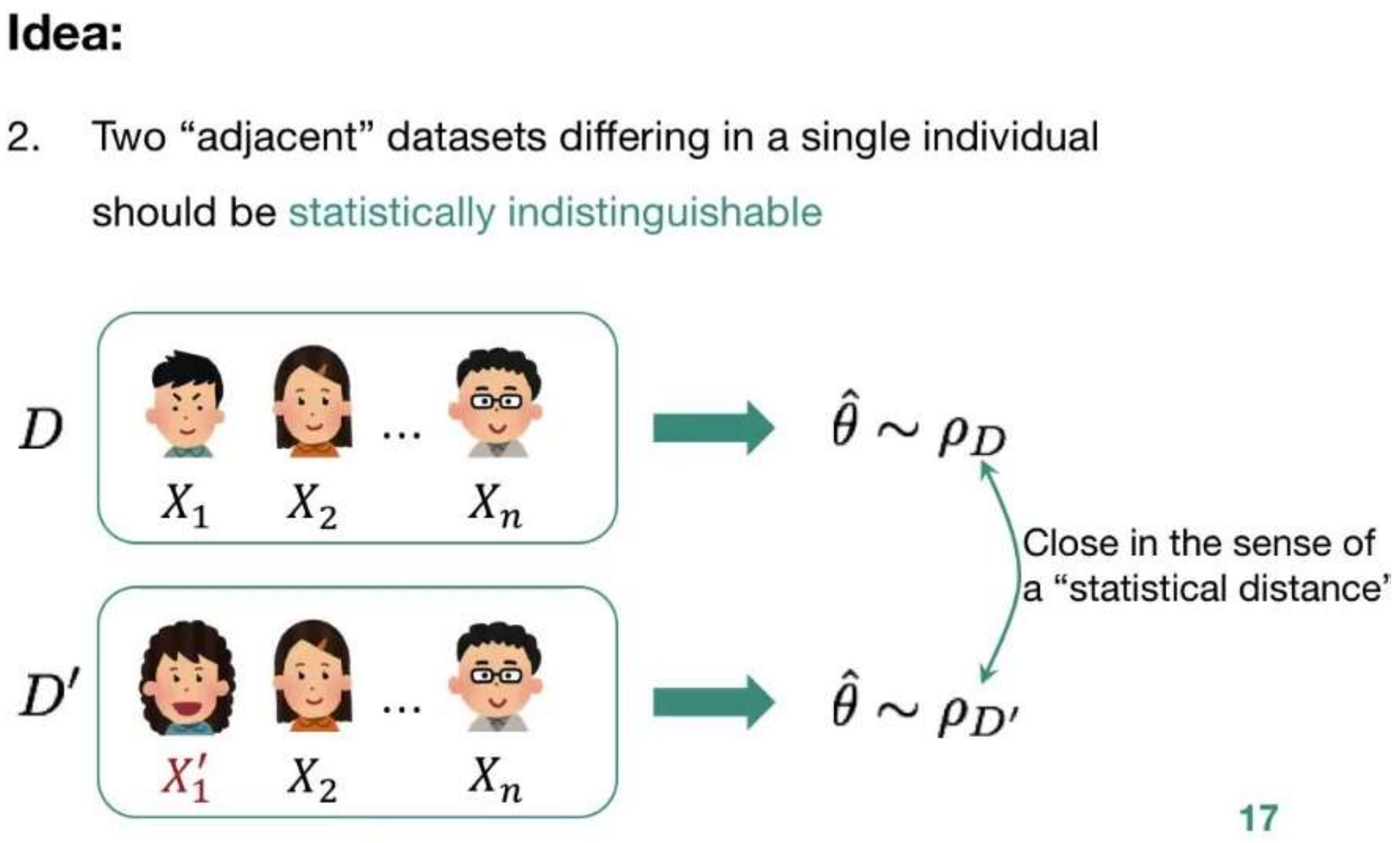
https://en.wikipedia.org/wiki/K-anonymity

Randomized Response

- Not really what is used, but it gives you the idea
- Flip a coin:
  - Heads means you tell the truth
  - Tails means you again flip a coin to give your answer

Differential Privacy

- Cynthia Dwork, Frank McSherry, Kobbi Nissim, Adam D. Smith



Idea:

2. Two “adjacent” datasets differing in a single individual should be statistically indistinguishable

Close in the sense of a “statistical distance’

17

Differential Privacy

- 2020 US Census data will be protected by differential privacy
    - https://privacytools.seas.harvard.edu/why-census-bureau-adopted-differential-privacy-2020-census-population

Current Issues in Web Security

- Code dependencies
  - What if there’s a bug in JQuery?
- Building a trustworthy browser
  - Brave, Epic, Firefox Focus
- How do we align online tracking with what users want?
- How do we align the actual security guarantees with users’ expectations?

Current Issues in Web Security

- Code dependencies
  - What if there’s a bug in JQuery?
- Building a trustworthy browser
  - Brave, Epic, Firefox Focus
- How do we align online tracking with what users want?
- How do we align the actual security guarantees with users’ expectations?

Current Issues in Software Security

- Automating bug-finding
  - Builds on fuzzing
- Software that is guaranteed secure by construction
- Eliminating side channels
- Trusted execution environments / Intel SGX
- Advanced persistent threats (APTs)
- How do we stop cryptojacking?

Current Issues in Usable Security

- Can we do better than notice & choice?
- How do we provide transparency?
- Are we shifting the burden to users?
- How do we reason about privacy / security over the long term?
  - Abandoned / forgotten-about resources
- Security in homes / sensing
- How do we achieve privacy by design?