Guest Lecture: Recent Privacy Legislation

Aleecia M. McDonald
Outline

• Sources of Internet law & policy
• CA AB 375
• GDPR
• Safe Harbor & Privacy Shield
Sources of Internet law & policy
International (or multi-national)

• Universal Declaration of Human Rights (UDHR)
• Fair Information Practice Principles (FIPPs)
• Standards bodies (W3C, IETF, ICANN…)
• European Union
• UN (International Telecommunication Union…).
Universal Declaration of Human Rights, 1948

• International Covenant on Economic, Social & Cultural Rights

• International Covenant on Civil and Political Rights

  • US signed in 1977, ratified in 1992, with five reservations

  • Article 17

1. No one shall be subjected to arbitrary or unlawful interference with his **privacy**, family, home or correspondence, nor to unlawful attacks on his honour and reputation.

2. Everyone has the right to the protection of the law against such interference or attacks.
Origin of the Fair Information Practice Principles

• HEW Report set out principles, 1973

• Concerns about mainframes and SSNs

1. There must be no personal data record-keeping systems whose very existence is secret.

2. There must be a way for a person to find out what information about the person is in a record and how it is used.

3. There must be a way for a person to prevent information about the person that was obtained for one purpose from being used or made available for other purposes without the person’s consent.

4. There must be a way for a person to correct or amend a record of identifiable information about the person.

5. Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuses of the data.
Standards Bodies: the W3C

- Tim Berners-Lee started in 1994 around HTML
- Platform for Internet Content Selection (PICS)
  - Used to strike down much of the Communications Decency Act
- Platform for Privacy Preferences (P3P)
- Do Not Track (DNT)
EU Privacy Directive: national implementations

- Privacy is a fundamental human right
- Protections mainly against corporations, not government
- ePrivacy (Directive 2002/58 on Privacy and Electronic Communications, as amended by Dir. 2009/136) - Article 5(3)

Member States shall ensure that the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information in accordance with Directive 95/46/EC, inter alia about the purposes of the processing, and is offered the right to refuse such processing by the data controller. This shall not prevent any technical storage or access for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network, or as strictly necessary in order to provide an information society service explicitly requested by the subscriber or user.
Netherlands’ ePrivacy Directive

• 2012 Amendment to the Telecommunications Act
  • Specific, informed consent for what data is collected and how it is used
  • Unique identifiers are presumed to entail the processing of personal data
United Kingdom’s ePrivacy Directive

- Implied consent; bury the terms in a privacy policy
- “Cookie shades”

The UK Information Commissioner’s Office, https://ico.org.uk

International Association of Privacy Professionals, http://www.privacyassociation.org
Spoiler Alert

Split led to GDPR, to be discussed in a few more slides
Additional EU privacy sources

- Data Protection Authorities
- Article 29 Working Party
- European Commission in Belgium
- European Court of Justice in Luxembourg
United States Sources of Privacy Law & Regulation

- Bill of Rights & case law
- Sectorial legislation
- Regulatory agencies
  - FTC
  - FCC
- “Industry self-regulation”
- White House
  - Commerce Department
  - Consumer Bill of Privacy Rights
  - State Attorneys General
  - State laws
Privacy in the Bill of Rights

- 1st Amendment: privacy of beliefs
- 3rd Amendment: privacy of the home not to house soldiers
- 4th Amendment: unreasonable searches
- 5th Amendment: self-incrimination
- 9th Amendment: enumeration does not deny other rights retained by the people
- 14th Amendment: no denying life, liberty, or property without due process of law
Griswold v Connecticut (1965)

- Court case example with agreement on privacy as the outcome, but very different legal reasoning

- Justice Douglas -> “*penumbras*” and "emanations" of the Bill of Rights creating “a zone of privacy”

- Justice Goldberg -> Ninth Amendment “other rights retained by the people”

- Justice Harlan -> Fourteenth Amendment's liberty clause; searching bedrooms is inconsistent with “the concept of ordered liberty.”
Word of the day: penumbra
State Constitutions, e.g. California

- Article 1, Section 1:

All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy.

- Added by Proposition 11, “Right of Privacy,” in Nov 1972
Patchwork of privacy

• “Sectorial approach” to privacy
  • Hard to come up with a one-size-fits-all approach to all data in all contexts
  • Protect certain people or types of data particularly

• The Internet is was allergic to laws
  • Early Libertarian / anti-authoritarian bent
  • Technologists feared legislative ignorance, aka unintended consequences
  • “Internet time” v. “I’m just a bill” and stifling innovation
  • Few big companies with power were regulated
A Few Examples of US Privacy Laws

- Fair Credit Reporting Act (1970)
- Video Privacy Protection Act (1988)
- Children's Online Privacy Protection Act (COPPA, 1998)
- California Shine the Light (2003)
- Do Not Call (2003)
Federal Trade Commission

- Consumer protection and online trust
- Holds hearings, convenes round tables, nudges research, writes reports
- Regulatory authority
  - Enforcement on the basis of deceptive or unfair practices
  - Consent decrees (e.g. Google, Facebook, Twitter)
Federal Communications Commission

- Parallel to the FTC
- Manages radio interference and media generally
- The Internet is carried by FCC-regulated entities
- Privacy generally left to FTC, but privacy appeared repeatedly in the National Broadband Plan during the Obama administration
Occasional White House involvement

- Individual control
- Transparency
- Respect for context
- Access and Accuracy
- Focused Collection
- Accountability
State Attorneys General

- Enforce state laws
- Technical investigations of privacy practices
- Advise companies of best practices (e.g. Privacy on the Go report)
- Informally advise the legislature

The California AG’s office brought suit against Delta et. al. for:

- Violating the 2004 California Online Privacy Protection Act
- Violating the California Unfair Competition Law
- Jurisdiction based on customers, not Delta’s headquarters in Atlanta
Why interfere with the free market?

- In a free market, users make decisions about whom to:
  - trust
  - do business with
  - have one-time or on-going interactions

- Why treat Internet privacy any differently?
  - Information asymmetries
  - Expect “market failure” as a result
Alternative to Free Market: Industry Self-Regulation

- Rather than government handling:
  - Legislation
  - Enforcement
  - Adjudication
- …industry creates own mechanisms
- Not great privacy successes
CA AB 375:
California Consumer Privacy Act
Unusual legislative history

• Alastair Mactaggart et. al. created a ballot initiative

• Ballot measure qualified; reported $3M of Mr. Mactaggart’s personal funds

• Polling around 80% support

• Committee to Protect California Jobs: Facebook, Google, Comcast, Verizon, and AT&T @ $200k each to start

• Minimal support for initiative from privacy organizations
Replaced the ballot measure with a bill

• Weaker on enforcement yet broader on what is covered

• Still little privacy organization support

• Law comes into force in 2020

• Next fights:
  • “Clean up” bill in CA
  • Federal preemption
California Consumer Privacy Act

To whom does the law apply? Any company world-wide with one or more:

1. Annual gross revenues over $25M

2. Holds personal information on 50,000 or more people / households / devices

3. 50% or more of annual revenue from selling consumers’ personal information

Jurisdiction is based on the consumer being in California.
What new rights does the law afford?

1. The right of Californians to know what personal information is being collected about them.

2. The right of Californians to know whether their personal information is sold or disclosed and to whom.

3. The right of Californians to say no to the sale of personal information.

4. The right of Californians to access their personal information.

5. The right of Californians to equal service and price, even if they exercise their privacy rights.

6. Also grants deleting data and data portability.

Details

• What is personal information?

  • “…identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Personal information includes, but is not limited to, the following:

    • Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier Internet Protocol address, email address, account name, social security number, driver’s license number, passport number, or other similar identifiers.”

• What’s a verifiable request from a consumer?
Many exemptions

• “Complete the transaction for which the personal information was collected, provide a good or service requested by the consumer, or reasonably anticipated within the context of a business’s ongoing business relationship with the consumer, or otherwise perform a contract between the business and the consumer.”

• Fraud

• Security

• Law enforcement

• Specific scientific research (not analytics per se)

• With consent
Enforcement (1 of 2)

• Minimal private right of action
  
  • Theft of unencrypted data “as a result of the business’ violation of the duty to implement and maintain reasonable security procedures”
  
  • “To recover damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident or actual damages, whichever is greater”
  
• Have to give companies 30 days to fix it (if possible)

• Have to give the AG’s office the option to enforce first
Enforcement (2 of 2)

• All other violations go through the AG’s office
  • Businesses get 30 days to fix problems
  • If not, “civil penalty of up to seven thousand five hundred dollars ($7,500) for each violation”
  • 20% of penalties go to AG’s office to offset enforcement costs
• Initial request: 57 positions and $11.5M annual budget
Why no love from team privacy?

• Wanted to opt in to data collection, not opt out
  • Problem: opt in likely would not survive court challenges

• Wanted stronger private right of action
  • Problem: this was key to getting a deal for companies to stand aside and let the bill pass into law

• Wanted something more like GDPR: more rights, more penalties, more limits on what companies can do
  • Problem: US limits government, not much on business
GDPR:
The General Data Protection Regulation
Key difference

• Directive
  • Must be enacted in national laws
  • Interpreted by national courts

• Regulation
  • Goes into force across all EU member nations
  • “One stop shop” assigns companies to one nation
Timeline (1 of 2)

- Directive enforcement starting October, 2003
  - Not well liked by industry. Mainly ignored or subverted.
  - UK’s Sliktide: “The idea of this law is a noble one, it's just a shame it was drafted by a team of technically illiterate octogenarians who couldn't find a button on a mouse.” Also, “Dear ICO, sue us.”
Timeline (1 of 2)

- General Data Protection Regulation 2016/679 in April, 2016

- GDPR enforcement in May, 2018

  - 14 years after the Directive which was fundamentally similar, yet companies complained bitterly that they did not have time to comply

- ePrivacy Regulation (ePR) is *lex specialis* to the General Data Protection Regulation; comes into force in 2019
US companies never thought GDPR would happen

• Submitted 3000+ proposed amendments

• Massive lobbying effort
  • Ex: US embassy in the Netherlands invited a PhD student to tea to change his mind on opt in v. opt out
  • Flat out denial that Do Not Track could help companies with GDPR compliance on the grounds that GDPR was speculative — even after the enforcement date
Example: Google

Non-personalized ads

Google will show all your users in the EEA only non-personalized ads.

*Non-personalized ads* are targeted using contextual information rather than the past behavior of a user. Although these ads don’t use cookies for ads personalization, they do use cookies to allow for frequency capping, aggregated ad reporting, and to combat fraud and abuse. **Consent is therefore required to use cookies [here](#) for those purposes from users in countries to which the EU ePrivacy Directive’s cookie provisions apply.**
GDPR Highlights (1 of 2)

• Fines can grow to €20 million or 4% annual sales, which ever is larger

• Jurisdiction based on person’s nationality, not company location

• Must have a “lawful basis for processing” — usually consent

• Duty for security, safeguards, breach notification

• Limited data retention

• Rights of access and erasure
GDPR Highlights (2 of 2)

• Setting cookies requires user consent *in advance*
  
  • Unless “strictly necessary for the delivery of a service requested by the user” and a few other exceptions
  
  • Browsers might be used, but not currently adequate to get user consent prior to setting cookies
Early results

From new CMU faculty member Timothy Libert, a study of news websites

**Third-party cookies per page by country** (April-July change in parenthesis)

- Average (-22%)
- United Kingdom (-45%)
- Poland (+20%)
- Italy (-32%)
- France (-32%)
- Finland (-19%)
- Spain (-33%)
- Germany (-6%)
Safe Harbor & Privacy Shield

Data transfer laws in 3 slides
Safe Harbor, 2000 - 2015

- US deemed “inadequate” because legal protections are not up to EU standards

- Under Safe Harbor, US companies pledged to do better than required by US law and self-certified they were up to EU protections for EU citizens

  - Enforcement: FTC

- Safe Harbor was struck down by EU courts, October 2015
Replaced by Privacy Shield, 2016 -> ???

- Fundamentally the same flaws: EU citizens have no privacy protections from US LEO
- This is not a problem individual companies can solve
- Patriot Act appears unlikely to be changed; FISA 702 authorized mass collection on all non-US citizens
- Recent EU review rather scathing:
  - Privacy and Civil Liberties Oversight Board has had quorum less than half the time; no recent appointments
  - No ombudsperson for EU complaints (no appointment)
  - FTC lacked commissioners (no appointments, then slow approval)
  - Facebook and Cambridge Analytica were covered by Privacy Shield
Predictions

• Second annual review in mid-October
  • European Parliament will complain that Privacy Shield is not protecting citizens
  • Grumpy press to follow, but no fundamental changes
• In contrast, the EU courts will throw out the Privacy Shield for the same reasons they threw out Safe Harbor
  • It is unclear what happens at that point
Guest Lecture: Recent Privacy Legislation

Aleecia M. McDonald