Standards Bodies: the W3C

- Platform for Internet Content Selection (PICS)
  - Used to strike down much of the Communications Decency Act
- Platform for Privacy Preferences (P3P)
  - “PICS for privacy”
- Do Not Track (DNT)
  - Five bills on DNT at the time W3C took it up
  - Request no tracking (DNT:0) or consent to tracking (DNT:1) with unset meaning keep collecting in US and stop collecting in EU

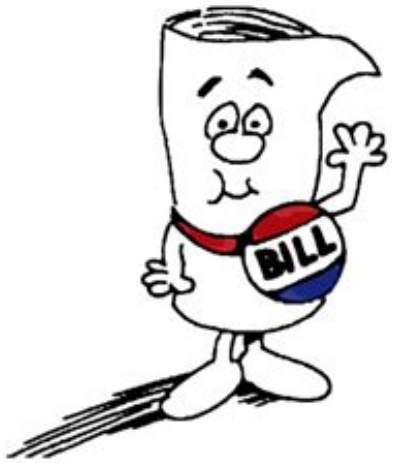
CA AB 375:
California Consumer Privacy Act

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.**

7. Over 16? Right to opt out. Under 16? Right to opt in.

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

Timeline (1 of 2)

- Directive 2002/58/EC in July, 2002
- 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 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