Day 5

Marketing/Personalization
Location Tracking
Right to be Forgotten
EU v US
1968 Crime Control Act
Targeted Ads

If you were shopping in person, sellers would know your gender and approximate age.

Entering a store = tacit informed consent to target you as a consumer?

Using a website = tacit informed consent to target you as a consumer?
Thanks for coming to Forbes. Please turn off your ad blocker in order to continue. To thank you for doing so, we’re happy to present you with an ad-light experience.
“You’re watching a 15-second Burger King ad, which is unfortunately not enough time to explain all the fresh ingredients in the Whopper sandwich,” the commercial’s actor says. He continues, “But I got an idea. O.K. Google, what is the Whopper burger?” Prompted by the phrase “O.K. Google,” the Google Home device next to the TV in the video lights up, runs a search and states its ingredients.
The right to be forgotten

- The right to have material removed.
- Negative right (a liberty)
- Positive right (a claim right)

Google Spain SL v. Agencia Española de Protección de Datos

Court of Justice of the European Union Creates Presumption that Google Must Remove Links to Personal Data upon Request.

http://harvardlawreview.org/2014/12/google-spain-sl-v-agencia-espanola-de-proteccion-de-datos/
Consumer Watchdog: Google Should Extend 'Right To Be Forgotten' to U.S.

by JAMES ENG
Right to be Forgotten
EU vs. US

- **EU’s rules are more strict than U.S. regulations**

- Citizens can request that any personal info indexed on Google that is “inadequate, irrelevant, or no longer relevant” be taken down.

- **EU Data Privacy Directive**
  - Prohibits transfer of personal information to countries outside the EU that do not have an adequate system of privacy protection. \( \rightarrow \) **Safe Harbor** plan
  - Update 10/2015 \( \rightarrow \) US no longer included in Safe Harbor after Snowden leaks reveal data storage
  - **Puts requirements on businesses outside the EU**
  - (See GDPR, slide 14 here and day 13 slides)
Late 2015

Facebook's Data Sharing Now In Danger After Safe Harbour Agreement Ruled Invalid By EU

The Huffington Post UK | By Thomas Tamblyn

Posted: 06/10/2015 11:01 BST | Updated: 06/10/2015 11:59 BST

Europe cracks down on U.S. tech with data ruling
CNNMoney - Oct 6, 2015

The court declared invalid a 2000 "Safe Harbor" agreement that allowed Facebook (FB, Tech30) and other tech firms to transfer users' data in ...

Europe's top court rejects 'Safe Harbor' ruling
USA TODAY - Oct 6, 2015

Europe Approves Tough New Data Protection Rules

By MARK SCOTT | DEC. 15, 2015
US options for removing Google search results

What Google product does your request relate to?  Web Search

What can we help you with?  I would like to remove my personal information from Google's search results

Our search results may contain a notice that some results have been removed.

Choose from the following options

- I would like to request that certain content about me that appears in Google’s search results in breach of European privacy law be removed
- I would like to remove my confidential, personal information from Google’s search results (e.g., security or government ID number, bank account or credit card number, or an image of your handwritten signature)
- I would like to ask the webmaster of a search result page which contains incorrect or inaccurate information to remove it completely from Google’s search results.
- My full name or the name of my business appears on an adult content site that's spamming Google’s search results
- I have located defamatory content in Google’s search results
Google & take down requests in the US

“Revenge porn” and Search

by Amit Singhal, SVP, Google Search

We've heard many troubling stories of “revenge porn”: an ex-partner seeking to publicly humiliate a person by posting private images of them, or hackers stealing and distributing images from victims’ accounts. Some images even end up on “sextortion” sites that force people to pay to have their images removed.

Our philosophy has always been that Search should reflect the whole web. But revenge porn images are intensely personal and emotionally damaging, and serve only to degrade the victims—predominantly women. So going forward, we’ll honor requests from people to remove nude or sexually explicit images shared without their consent from Google Search results. This is a narrow and limited policy, similar to how we treat removal requests for other highly sensitive personal information, such as bank account numbers and signatures, that may surface in our search results.

In the coming weeks we’ll put up a web form people can use to submit these requests to us, and we’ll update this blog post with the link.

We know this won’t solve the problem of revenge porn—we aren’t able, of course, to remove these images from the websites themselves—but we hope that honoring people’s requests to remove such imagery from our search results can help.

UPDATE, 7/9/2015: People can use this webform to submit revenge porn removal requests.

http://googlepublicpolicy.blogspot.com/2015/06/revenge-porn-and-search.html
General Data Protection Regulation

- Harmonize data rules across EU and for EU customers
  - American companies with EU users also must comply

- Basically, fair info principles become “regulation”
  - Major fines for noncompliance (10m euro)
  - Possible jail time if other laws are also broken + higher fines (20m)

- Data Protection Officers must be appointed
  - For companies of all sizes, not just large companies

- Explicit consent required for data profiling

1934 Communications Act prohibited interception of citizen’s messages w/o warrant

**1968 OMNIBUS CRIME CONTROL AND SAFE STREETS ACT** prohibits GOVERNMENT agencies from wiretapping

→ (Made the Katz decision (1967) into law)

Before ECPA → 3rd party doctrine → sharing info with a 3rd party (like an ISP) means you relinquish some rights to it. Gov’t no longer needs warrant, just prior notice.

**ELECTRONIC COMMUNICATIONS PRIVACY ACT** of 1986 (ECPA) extended the 1968 wiretapping laws to include electronic communications

→ **Title II: Stored Communications Act**: restricts gov’t and business access to e-data (gave 4th amendment level protection for data stored with ISPs)
Update: ECPA amendment proposed 9/2015

What is the biggest change that ECPA Amendments Act would make?

The bill adds a warrant requirement for communications that were previously considered so old as to be irrelevant to their participants and unworthy of privacy protections.

Right now, emails and other electronic messages older than 180 days are considered to have been “abandoned” by the people who sent and received them. Law-enforcement agencies don't need to get a warrant to force a company like Google or Facebook to turn over those communications. Agencies just need to assert in writing that they need the communication to further an active investigation.

2/2020: Still no progress.

Amended ECPA: requires telecom equipment be designed to ensure that the gov’t can intercept telephone calls (with a court order or other authorization). Has been upheld in several law suits.

Many are also passing data retention laws, forcing companies to retain information on their customers. In the U.S., the 1994 Communications Assistance for Law Enforcement Act required phone companies to facilitate FBI eavesdropping, and since 2001, the National Security Agency has built substantial eavesdropping systems with the help of those phone companies.

Systems like these invite misuse: criminal appropriation, government abuse and stretching by everyone possible to apply to situations that are applicable only by the most tortuous logic. The FBI illegally wiretapped the phones of Americans, often falsely invoking terrorism emergencies, 3,500 times between 2002 and 2006 without a warrant. Internet surveillance and control will be no different.
The National Security Agency (NSA)

“CALEA on steroids”
Intelligence gathering agency

0 1952: Formed to intercept and decode WW2 messages, only allowed to spy on foreign entities

0 **Patriot Act (2001)**: [Sec. 215] “the entirety of US communications may be considered relevant to a terrorism investigation if it is expected that even a tiny minority may relate to terrorism” ⇒ US now included in NSA surveillance... but most civilians were unaware (until 2013). Main surveillance provisions EXPIRED: June 1, 2015 ⇒ USA freedom act

Textbook p. 116-119
Update: 6/3/2015

**USA Freedom Act** signed into law

- Responds to expiration of Patriot Act (June 1, 2015)
- Extends most of Patriot Act until 2018.

- “Ended” bulk data collection by government, now it’s up to ISPs & telecom companies to collect data.
- Government agencies once again need warrants in order to request access to the records from the telecom companies.... International calls and emails not included (can still be collected).
Update: 1/2018

Congress votes to give NSA 6 more years of spying on Americans without a warrant

FOREIGN INTELLIGENCE SURVEILLANCE ACT (FISA) 1978:

- established oversight court for the NSA
- Both are government entities
- Judges appointed, not elected
- Aggregate numbers submitted to congress once/year.
- Section 702 of FISA update in 2008 allows for warrantless surveillance of Americans online.

"Quis custodiet ipsos custodes?" – Juvenal

- 2013: Snowden leaked evidence of NSA spying on millions of US citizens
- Utah Data Center: electricity = $3.3 million/month

See: https://en.wikipedia.org/wiki/United_States_Foreign_Intelligence_Surveillance_Court
FISA update 2008

Section 702: explicitly allowed, but placed more limits on, government spying

- yet each limit includes phrases like “unless necessary” or “as decided by FISA court”

- Extends whistleblower protections
  - But only in cases of “lawful disclosure,” only prevents “personnel action,” (wb’s can still be criminally prosecuted).

- Expired Dec, 2017
- Renewed Jan, 2018

The CLOUD Act

Allows police at home and abroad to seize cross-border data without following the privacy rules where the data is stored.

1. The Act expressly provides that U.S. law-enforcement orders issued under the Stored Communications Act (SCA) may reach certain data located in other countries.
2. The Act also allows certain foreign governments to enter into new bilateral agreements with the United States that will prequalify them to make foreign law-enforcement requests directly to U.S. service providers, rather than via the U.S. government under a mutual legal assistance treaty. This should streamline compliance with foreign law-enforcement requests.
3. The Act formalizes the process for companies to challenge a law enforcement request.
4. The Act imposes certain limits and restrictions on law enforcement requests to address privacy and civil liberty concerns.

NATIONAL SECURITY

Your TV Is Looking At You — The CLOUD Act and the Threat to Our Privacy Rights

BY RENE SOTOLONGO · AUGUST 26, 2018

RULE 41

0 Set procedural guidelines for courts (what time they open, which holidays the courts are closed, etc.)

0 The DOJ wants to “update” Rule 41 with extensive surveillance permissions for law enforcement
  0 Hiding one’s ID online would constitute probable cause for a warrant to remotely hack the computer
  0 Any computer that is part of a botnet system would be fair game for surveillance and remote hacking

0 This type of law usually must go through congress/be debated/have public input

0 Update 12/2016: Changes approved

https://www.eff.org/deeplinks/2016/04/rule-41-little-known-committee-proposes-grant-new-hacking-powers-government