Day 5

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

1986 ECPA
CALEA
NSA
FISA
Rule 41
Targeted Ads

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

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

0 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.
As Identity Concerns Reach An Inflection Point, The Weather Company Leans Into Subscriptions

by Sarah Sluis // Monday, March 22nd, 2021 – 12:30 am
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/
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.
content from websites that host it. The page may still exist on the website and this means it can be found through the URL to the website, social media sharing, or other search engines. We recommend reaching out to the website owner to request removal.

Access [this page](https://support.google.com/legal/troubleshooter/1114905?hl=en#ts=1115648) to learn more about how to contact a website owner.

What can we help you with?

- I would like to report malware, phishing or similar issues
- A piece of content I am concerned about has already been removed by the webmaster but still appears among the search results
- **Right to be Forgotten**: request to delist information per European data protection laws
- **Intellectual property issue**: report copyright infringement, circumvention, etc.
- **Other legal issue**: report content for a legal reason not already listed
Boston Globe launches ‘Fresh Start’ initiative: People can apply to have past coverage about them reviewed

Similar to “right to forget” programs that have cropped up across the country, the undertaking is meant to address the lasting impact that stories about past embarrassments, mistakes, or minor crimes, forever online, can have on a person’s life.

Jan 2021
General Data Protection Regulation

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

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)

https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1285
COMMUNICATIONS ASSISTANCE FOR LAW ENFORCEMENT ACT (CALEA) 1994

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 lawsuits.

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.

CNN.com, 2010
The National Security Agency (NSA)

“CALEA on steroids”
Intelligence gathering agency

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

o **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 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).

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

(FISA)

Update March 2020 (amid pandemic)

USA FREEDOM reauthorization act fails

Mitch McConnell tries to extend (expired!) Sec 215 of Patriot Act

Not enough votes; does not pass (for now...)

January 2023:

Section 702 was first added to FISA in 2008 and renewed for six years in 2018, when Trump originally tweeted opposition to the program but then reversed himself.

Nakasone argued the law "plays an outsized role in protecting the nation" and generates "some of the U.S. government's most valuable intelligence on our most challenging targets."

He gave several broad examples of that work, including the discovery of attempts to steal sensitive U.S. technology, stopping the transfer of weapons components, preventing cyberattacks, and "understanding the strategic intentions" of China and Russia.

"We have saved lives because of 702," Nakasone told a virtual meeting of the U.S. Privacy and Civil Liberties Oversight Board.

NSA Director Pushes Congress to Renew Surveillance Powers


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
Utah
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).

- “Incidental” surveillance of US citizens is allowed in the scope of non-US investigations.

- Expired Dec, 2017
- Renewed Jan, 2018

statement by the president on FISA Amendments Reauthorization Act of 2017

Today, I signed into law S. 139, “FISA Amendments Reauthorization Act of 2017” (the “Act”). The Act reauthorizes Title VII of the Foreign Intelligence Surveillance Act until December 31, 2023, and makes a number of amendments to current law. Section 702 of Title VII allows the Intelligence Community, under a robust regime of oversight by all three branches of Government, to collect critical intelligence on international terrorists, weapons proliferators, and other important foreign intelligence targets located outside the United States.
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.

A BILL

To amend title 18, United States Code, to improve law enforcement access to data stored across borders, and for other purposes.

1. Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled, and

SECTION 1. SHORT TITLE.

This Act may be cited as the “Clarifying Lawful Overseas Use of Data Act” or the “CLOUD Act”.

SEC. 2. CONGRESSIONAL FINDINGS.

Congress finds the following:

Passed 2018
Set procedural guidelines for courts (what time they open, which holidays the courts are closed, etc.)

The DOJ wants to “update” Rule 41 with extensive surveillance permissions for law enforcement

- Hiding one’s ID online would constitute probable cause for a warrant to remotely hack the computer
- Any computer that is part of a botnet system would constitute probable cause for a warrant to remotely hack the computer

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

Update 12/2016: Changes approved