# Privacy

INFO 200

Part II

**Joseph Janes**
**Associate Professor, Information School**

# Privacy 2
## agenda

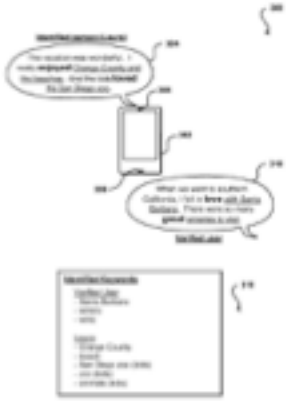
- contemporary threats to privacy
- your friends & what to do

ABC NEWS VIDEO LIVE SHOWS

## Amazon patent reveals 'voice sniffer algorithm' that could analyze conversations

The algorithm may analyze "trigger words" to find likes and dislikes of a user.

***Hey, Alexa, What Can You Hear? And What Will You Do With It?***



PRIVACY & SECURITY

## As Amazon Looks To Unlock Your Door, Taking Stock Of Meaning Of Privacy

November 8, 2017 · 9:28 PM ET

Heard on All Things Considered

***Most White Americans' DNA Can Be Identified Through Genealogy Databases***

## How to Identify Almost Anyone in a Consumer Gene Database

New techniques that dig more deeply into genetic databases may soon make the anonymity of their customers' DNA impossible to safeguard

NATIONAL

**Don't want the police to find you through a DNA database? It may already be too late.**

GeekWire NEWS JOBS EVENTS RESOURCES ABOUT Search

Trending: Former spouse's allegations against Portland startup CEO ripple through tech community

## Safety over privacy? RealNetworks to offer free facial recognition technology to K-12 schools

## *YouTube Is Improperly Collecting Children's Data, Consumer Groups Say*

## 'You can track everything': the parents who digitise their babies' lives

Socks that record heart rate and cots that mimic the womb might promise parents peace of mind – but is the data given to tech firms a fair exchange?

## The University of Arizona Tracked Students' ID Card Swipes to Predict Who Would Drop Out

## Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret

Dozens of companies use smartphone locations to help advertisers and even hedge funds. They say it's anonymous, but the data shows how personal it is.

By JENNIFER VALENTINO-DeVRIES, NATASHA SINGER, MICHAEL H. KELLER and AARON KROLIK DEC. 10, 2018

No Cash Needed At This Cafe. Students Pay The Tab With Their Personal Data

## The secret data collected by dockless bikes is helping cities map your movement

Lime and other companies are gathering masses of location-based information that some cities are leveraging to improve their streets.

AP

## AP Exclusive: Google tracks your movements, like it or not

SAN FRANCISCO (AP) — Google wants to know where you go so badly that it records your movements even when you explicitly tell it not to.

An Associated Press investigation found that many Google services on Android devices and iPhones store your location data even if you've used a privacy setting that says it will prevent Google from doing so.

Opinion

## Amazon Wants to Get Even Closer. Skintight.

In the pursuit of surveillance as a service, Jeff Bezos is intent on recording even our moods. How much personal data is too much to give to Amazon?

By Kara Swisher
Contributing Opinion Writer

Halo is Amazon's attempt to compete with the Apple Watch and Google (which is awaiting approval of its acquisition of Fitbit) in the health-tracking arena. I got on the wait list for it as soon as it was introduced in the summer, and it arrived on Halloween. I strapped on the attractive band and turned on all the intrusive bells and whistles, which Amazon had trumpeted as good for me.

That first day a vexed emoji told me I was "stern" or "discouraged" for 16 percent of the day. "You had one phrase that sounded restrained and sad" for 1.6 seconds at 12:30 p.m., it reported, although I have no idea what that phrase could have been. But 8 percent of the day, including for 14.4 seconds at exactly 11:41:41 a.m., I was "satisfied," with "two phrases that sounded satisfied, delightful or appreciative." Later, for 1.2 seconds at 7:18:30 p.m., I was "afraid, panicked or overwhelmed."

# Big data meets Big Brother as China moves to rate its citizens

WIRED

The Chinese government plans to launch its Social Credit System in 2020. The aim? To judge the trustworthiness – or otherwise – of its 1.3 billion residents

## nothing new

The New York Times

NEW YORK, THURSDAY, SEPTEMBER 6, 2001

TRACKS IN CYBERSPACE

### Government Wary Of Laws on Privacy

Washington is not creating new laws and regulations that might restrict the use of cookies and other high-technology tools by businesses to monitor Internet users' activities.

Some lawmakers say that the politics of privacy is so sensitive and complex that a deliberate approach is best — but there is growing agreement that some kind of government action will eventually have to emerge.

## contemporary threats to privacy (EFF)

EFF 30 ELECTRONIC FRONTIER FOUNDATION

PRIVACY TOPICS

BIOMETRICS
KNOW YOUR RIGHTS
INTERNATIONAL PRIVACY STANDARDS
MANDATORY DATA RETENTION
ANONYMITY
ARTIFICIAL INTELLIGENCE & MACHINE LEARNING
BORDER SEARCHES
CALEA
CELL TRACKING
COVID-19 AND DIGITAL RIGHTS
CYBER SECURITY LEGISLATION
DECODING 702: WHAT IS SECTION 702?
DIGITAL BOOKS
DO NOT TRACK
ELECTRONIC FRONTIER ALLIANCE
ENCRYPTING THE WEB
FACE SURVEILLANCE
LOCATIONAL PRIVACY
MEDICAL PRIVACY
MOBILE DEVICES
NATIONAL SECURITY LETTERS
NSA SPYING
NSL
ONLINE BEHAVIORAL TRACKING
OPEN WIRELESS
PATRIOT ACT
PEN TRAP
PRINTER TRACKING
REAL ID
RFID
SEARCH ENGINES
SEARCH INCIDENT TO ARREST
SOCIAL NETWORKS
STREET-LEVEL SURVEILLANCE
STUDENT PRIVACY
SURVEILLANCE DRONES
TRAVEL SCREENING
SURVEILLANCE TECHNOLOGIES

## contemporary threats to privacy (EFF)

tracking
user data protection
facial recognition
search engines
mass surveillance
social networks
cloud education services & devices in school
travel screening/border searching

*all of the next several slides are selected examples and quotes from Electronic Frontier Foundation website eff.org*

## tracking

Countless advertising networks are able to secretly monitor you across multiple websites and build detailed profiles of your behavior and interests

**cookies** allow sites to store a unique ID in your browser, and therefore to track you—and if a company is present on multiple websites, it can track your visits to each of those sites. In other words, a company can use cookies to construct a detailed overview of users' activity

**supercookies & fingerprints** follow people who try to delete their cookies, and the **leakage of user IDs** from social networks and similar sites has often given them an easy way to identify the people they were tracking.

**https://coveryourtracks.eff.org/**

## mass surveillance

For years, there's been ample evidence that authoritarian governments around the world are relying on technology produced by American, Canadian, and European companies to facilitate human rights abuses. From software that enables the filtering and blocking of online content to tools that help governments spy on their citizens, many such companies are actively serving autocratic governments as "repression's little helper."

The reach of these technologies is astonishingly broad: **governments can** listen in on cell phone calls, use voice recognition to scan mobile networks, read emails and text messages, censor web pages, track a citizen's every movement using GPS, and can even change email contents while en route to a recipient. Some tools are installed using the same type of malicious malware and spyware used by online criminals to steal credit card and banking information. They can secretly turn on webcams built into personal laptops and microphones in cell phones not being used. And all of this information is filtered and organized on such a massive scale that it **can be used to spy on every person in an entire country**.

## locational privacy

**Modern communications mean most individuals today walk around with a beacon that transmits their location.**

Mobile phones register to a nearby tower as the owner moves through space and the phone company can collect that data in real time or retrospectively to physically place the phone with varying degrees of accuracy. GPS enabled phones enable far more precise location placement.

Many cars now have GPS devices installed some of which transmit the vehicle's location to a centralized service. As the devices get cheaper and smaller law enforcement agencies can more easily attach GPS trackers to cars and individuals enabling precise round-the-clock surveillance without ever leaving the precinct.

## user data protection

Uber, Airbnb, Lyft, TaskRabbit, Instacart, etc

To access the services offered, or to offer services via company apps, individuals are disclosing data about **where they live and shop, what they buy, where they sleep, and where they travel**

aren't promising to stand by their users: half of the companies reviewed **didn't require a warrant** before turning over customer data to law enforcement.

Choosing "Always" enabled Uber to **track your location for five minutes** after you leave the vehicle

Microsoft Windows 10: a non-exhaustive list of data sent back: location data, text input, voice input, touch input, webpages you visit, and telemetry data regarding your general usage of your computer, including which programs you run and for how long

Evernote adopted a new privacy policy in December 2016 that allows some employees to **read user content** for the sake of improving its machine learning technology

## facial recognition

Law enforcement use of face recognition technology poses a profound threat to personal privacy, political and religious expression, and the fundamental freedom to go about our lives without having our movements and associations covertly monitored and analyzed.

This technology can be used for identifying or verifying the identity of an individual using photos or videos, and law enforcement and other government agencies can use it to conduct dragnet surveillance of entire neighborhoods. Face surveillance technology is also prone to error, implicating people for crimes they haven't committed.

It has been well documented by MIT, the Georgetown Center for Privacy and Technology, and the ACLU that these **error rates—and the related consequences—are far higher for women and people with darker skin.**

## search engines & browser histories

record your search queries and maintain massive databases that reach into the most intimate details of your life

## cloud education services & devices in schools

Almost one third of all students already use school-issued digital devices

When students log into Google, whether through Chromebooks or through GAFE, Google collects a **huge variety of personal data by default**: search history and which results students click on, videos they search for and watch on YouTube, usage data and preferences, Gmail messages, G+ profiles and photos, docs, and other Google-hosted content and content that flows through Google's systems.

Additionally, if students use Chrome (the only browser available on Chromebooks), Google also collects the following information **by default**: browsing history, bookmarked URLs, passwords, website form entries, and which extensions are installed—and Google stores this information in the **cloud** (rather than locally on the Chromebook itself).

## travel screening/border searching

increasing use of biometric (fingerprint, facial recognition, retinal/iris scan) technologies for tracking of travelers, including in all areas of airports, border crossings, boarding, luggage check (with cooperation of some airlines), including maintenance and storage of this data for up to 75 years

partnering with companies that do concert and stadium security/ entry

marked increase in searches of cell phones and other electronic devices by border agents (without warrant or probable cause), including confiscation and examination (warrants are required for police to search phones of people arrested)

## what to do

## your friends: Europe/"right to be forgotten"

European (EU) citizens can request that Google and other search companies remove links to private information about them, on request, provided the information is no longer relevant (European Court of Justice, *Google v. Spain*, 2015)

"The Court found that the fundamental right to privacy is greater than the economic interest of the commercial firm and, in some circumstances, the public interest interest in access to Information." (EPIC)

https://www.google.be/intl/en/policies/faq/

## your friends: Europe/GDPR

**General Data Protection Regulation** "to protect all EU citizens from privacy and data breaches in today's data-driven world" (eugdpr.org)

- increased territorial scope (companies/orgs doing business in EU)
- companies in breach can be fined to 4% of annual turnover/€20M
- rules for consent of use of data must be clear, accessible, with purposes of data processing
- breach notification (EU citizens) 72 hours
- right of access to what is being processed, where, and why, incl. free copy of data
- privacy by design (hold only data absolutely necessary)
- companies must have Data Protection Officer

## your friends: US public libraries

shield laws for circulation records, browsing histories, database and search engine use, attendance at programs, etc

## your friends: US Federal Law/HIPAA

creates national standards to protect individuals' medical records and other personal health information.

It gives patients more control over their health information, sets boundaries on the use and release of health records, establishes appropriate safeguards that health care providers and others must achieve to protect the privacy of health information.

And it strikes a balance when public responsibility supports disclosure of some forms of data – for example, to protect public health.

It enables patients to **find out how their information may be used**, and about certain disclosures of their information that have been made.

It generally **limits release of information to the minimum reasonably needed** for the purpose of the disclosure.

It generally gives patients the **right to examine and obtain a copy of their own health records and request corrections**.

It empowers individuals to **control certain uses and disclosures** of their health information.

https://www.hhs.gov/hipaa/for-individuals/faq/187/what-does-the-hipaa-privacy-rule-do/index.html

## your friends: US Federal law/FERPA

protects the privacy of student education records

rights include:

The right to inspect and review the student's education records

The right to request the amendment of the student's education records that the student believes are inaccurate, misleading, or otherwise in violation of the student's privacy rights under FERPA. (*This process cannot be used to challenge a grade.*)

The right to provide written consent before the University discloses personally identifiable information from the student's education records, except to the extent that FERPA authorizes disclosure without consent.

https://registrar.washington.edu/students/ferpa/

## your other friends

journalists

lawsuits

geeks

shareholders/market pressures/societal pressure

## what to do

know what's happening

pay attention

take precautions (privacy settings/notifications, HTTPS, VPNs, etc.)

advocacy

build privacy in to designs

The New York Times

## *Facebook's Mark Zuckerberg Says He'll Shift Focus to Users' Privacy*

Mark Zuckerberg, Facebook's chief executive, said he planned to build systems and products that create a type of "digital living room" where people can expect their discussions to be private. Eliot Blondet/SIPA, via Associated Press

## a final word

"…if we cannot control who has access to us,…then we cannot control the patterns of behavior we need to adopt or the kinds of relations with other people that we will have."

Rachels. "Why Privacy is Important". 1975