Your Digital Privacy

Howard Fosdick © 2024
This is licensed...

- Distribute this talk
- But do not alter it

Transcript and Slides: [https://rexxinfo.org/howard_fosdick_articles/index_fosdick_articles.html](https://rexxinfo.org/howard_fosdick_articles/index_fosdick_articles.html)

Turn off recording devices

The Full License: [https://creativecommons.org/licenses/by-nd/4.0/](https://creativecommons.org/licenses/by-nd/4.0/)
Who am I?

Independent Computer Consultant

- Database & Systems
- Author of books & many articles
- Thinker
Agenda

I. What is Privacy?
II. Technologies
III. Gov’t Surveillance
IV. Solutions

Focus is on privacy problems
What is Privacy?

1980s    1990s    2000s    Today

Analog

Digital

Surveillance
Society

Communications:
- texting, email
- phone, voip
- documents

Activities:
- all devices collect data
- purchases
- everywhere you go
- entertainment
- internet (searches, websites)

Personality:
- social media
- posts (UTube, forums, blogs)
- behaviors

Who controls data about you?
Privacy is *Power*

1. Information is power
2. Privacy is about who controls information about you
3. Therefore, Privacy is power
4. Control of your data yields more control over your life!

© H. Fosdick
Privacy is *Power*

Example: Salary Negotiation

Without privacy, you lose!

Do they know your salary:
- [www.nbcnews.com/technolog/exclusive-your-employer-may-share-your-salary-equifax-might-sell-1B8173066](http://www.nbcnews.com/technolog/exclusive-your-employer-may-share-your-salary-equifax-might-sell-1B8173066)
Privacy is a Human Right

Psychology: Privacy is required for the existence of the self

A Human Right:

Read: www.humanrightscareers.com/issues/is-privacy-a-human-right/
Is Your Privacy Protected From Corporations?

Courtesy: Forrester Research, ZDNet.com, and Forbes.com  (old slide but accurate for US)
Surveillance Capitalism appropriates your data for conversion into an intimate understanding of you.

Your data drives profits!

A $230 billion business!

-> a new Gold Rush


Source: Transparency Market Research 2023
Is Your Privacy Protected From the Government?

Surveillance By:
UK  Democracy
USA  Secrecy

International Privacy Index
- Endemic surveillance societies
- Extensive surveillance societies
- Systemic failure to uphold safeguards
- Some safeguards but weakened protections
- Adequate safeguards against abuse
- Significant protections and safeguards
- Consistently upholds human rights standards

Courtesy: Privacy International, EPIC, and BestVPN
(old slide but accurate for USA & UK)
US Gov’t Surveillance

Executive Branch Top Secret --
Congress, Judiciary, and public are in the dark

10 years ago:
- Budget $75B + black budget
- 1.7B communications stored per day
- 1,271 agencies
- 1,931 contractors
- 1 million have top-secret clearance

“Collect it all.” --former NSA Director Keith Alexander

Read - www.pbs.org/newshour/show/nsa-collects-word-for-word-every-domestic-communication#transcript  
https://en.wikipedia.org/wiki/Mass_surveillance#United_States  
www.aclu.org/issues/national-security/privacy-and-surveillance/nsa-surveillance  
www.theguardian.com/world/2021/sep/04/surveillance-state-september-11-panic-made-us-vulnerable
New York Times’ Privacy Project

Here is the stark truth: We in the West are building a surveillance state no less totalitarian than the one the Chinese government is rigging up.

How US Surveillance Happened

1975 to 2001: FBI – domestic / NSA – overseas

2001: Bush – NSA targets America to find thousands of Al-Qaeda “sleeper agents”

2016: Obama – 16 agencies get NSA data

Data used for purposes other than fighting terrorism

Unconstitutional – 4th Amendment

Status Today?

Read: www.theguardian.com/world/2021/sep/04/surveillance-state-september-11-panic-made-us-vulnerable

www.privacyjournal.net/edward-snowden-nsa-prism/
Why You are Losing Privacy

1. Your life is digitized
2. They gain power by appropriating your data
Privacy Misconceptions

- I'm not important, they won’t bother with me
  - Why is your data a $230 billion industry?
- They won’t notice me... I’ll hide in the crowd
  - Computers process billions of records equally
- I don’t care if they target me for ads
  - This is about power to manipulate you
- You have no privacy, get over it
  - Laws can fix this!
- If you have nothing to hide, you have nothing to fear
  - “Give us power without oversight – just trust us!”
II. Technologies

← Recommended
Tracking Your Location

Location Tracking Technologies:

- Cellphones
- Cars
- Wearables
- License Plate Readers (LPRs)
- GPS
- Geofencing
- Stingray (govt tool)
- Cameras (Facial Recog. soon)
  - Home (Ring)
  - Streets
  - Schools
  - Stores
  - Events
  - Cars
- Aerial
  - Gorgon Stare
  - Satellites
  - Drones
  - Planes

You’re tracked 24 x 7 x 365!

Selling your data is a $12 Billion business

Cell Tracking –
Reports your location tens of thousands of times per day!

Why Do You Care?

Location data tells –

- If you’re LGBTQ
- Your race & ethnicity
- Your medical problems
- If you’re in therapy
- If you drink a lot
- If you cheat on your spouse
- Who you sleep with
- If you’re hiding taxable income
- Political beliefs
- If you oppose US military policies
- How you vote
- If you’re a religious minority
  … so much more ...

Data Appropriation:

Do we want private lives?

Or do we let corporations sell them?

Read
http://ssd.eff.org/en/module/problem-mobile-phones
https://en.wikipedia.org/wiki/Carpenter_v._United_States
https://themarkup.org/privacy/2021/09/30/theres-a-multibillion-dollar-market-for-your-phones-location-data

Principle: “Big Data” tells them anything!
Facial Recognition

Your face is appropriated:
- Internet
- Social Media
- Youtube
- Govt IDs
- Airports
- etc

- Data Cross-Use
- Future Use

Your face is a password you can’t change

FR Evolution

video analytics
real-time
static

Read:
- www.pogo.org/analysis/2021/08/key-facts-about-face-recognition-for-policymaking
- www.aclu.org/news/privacy-technology/fbi-has-access-over-640-million-photos-us-through
- www.siliconrepublic.com/enterprise/facial-recognition-technology-concerns-problems
- www.theguardian.com/technology/2019/jul/29/what-is-facial-recognition-and-how-sinister-is-it
Drivers Privacy Protection Act (1994, 2020) is ineffective.

Where You Live

- National ID
- State ID
- Biometrics

Biometrics

- Where You Live

- National ID
- State ID
- Biometrics

1. Over Collection
2. Cross Use
3. Ineffective Laws

- Buy liquor, cigarettes
- Bar
- Mail a package
- Airport
- Filming taxes
- Employers
- Buy or rent a car
- Police
- Return store item
- Hospital
- Border
- Bank
- Purchase over $10k

Drivers Privacy Protection Act (1994, 2020) is ineffective.
(1) The more you give out your data, the more you’ll pay (eg, ID theft)

(2) But you’re often *forced* to give out your data

(3) Then it’s sold! Or hacked!

(4) You can’t connect how it harms you to who is responsible

(5) This is why people don’t “get” privacy

Privacy? I don’t see that we have a problem...
Public Surveillance – Ring

Courtesy: Amazon Ring

Surveils the street  
Listens to 40 feet

Neighbors app
LEA (police) partnership
Facial Recognition?  
AI?

Read – eff.org/deeplinks/2020/01/ring-doorbell-app-packed-third-party-trackers  
www.wired.com/story/why-we-do-not-recommend-ring/  
A comprehensive public surveillance network. It’s also a GOVERNMENT surveillance network.

- 1 Camera for every 4 Americans
  - Streets
  - Homes
  - Stores
  - Corporations
  - Google Streetview
  - Events
  - Schools (>90% for H.S. and M.S.)
- LEA partnerships
- Camera apps (like Neighbors)

Increase in surveillance cameras installed in the US

Security camera installations are up over 3,500% from 2004 to 2021

Source: Guardian 9/4/21

Read:
- www.safehome.org/doorbell-cameras/statistics/
The “Gorgon Stare” – Mass Aerial Surveillance

By:
- Police
- FBI
- DHS
- Military

Surveillance of entire city by one airborne vehicle

- No informing the public
- No community control
- Little evidence of crime reduction

--> Status?
Why Don’t Courts Protect Privacy?

Old precedents bind the courts:

No expectation of privacy in a public place

1967, 1976

=> Facial recognition, locational tracking ...

3rd Party Doctrine – You give out data, you lose control of it ... entirely

1967

=> No limits on use of your data

“The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated ... no Warrants shall issue, but upon probable cause ... describing the place to be searched, and the persons or things to be seized.”

4th Amendment

=> Forbids mass gov’t surveillance, and FISA court killed it
no fundamental right to privacy → scandal → a specific law
<table>
<thead>
<tr>
<th>Law</th>
<th>Problem</th>
<th>Read</th>
</tr>
</thead>
<tbody>
<tr>
<td>HIPAA (healthcare)</td>
<td>Only covers (1) Providers &amp; (2) Insurers</td>
<td><a href="http://www.propublica.org/article/health-insurers-are-vacuuming-up-details-about-you-and-it-could-raise-your-rates">www.propublica.org/article/health-insurers-are-vacuuming-up-details-about-you-and-it-could-raise-your-rates</a></td>
</tr>
<tr>
<td>GINA (DNA discrimination)</td>
<td>Only covers (1) Employment &amp; (2) Health Insurance. Nothing else!</td>
<td></td>
</tr>
<tr>
<td>GLBA Graham-Leach-Bliley Act (financial)</td>
<td>Opt-in is default. Consent forms are dark patterns</td>
<td></td>
</tr>
<tr>
<td>Credit Bureaus (financial) (FCRA), FACTA.</td>
<td>Credit theft is easy. Good: Consumer remediation</td>
<td></td>
</tr>
<tr>
<td>Childrens Online Privacy Protection Act (COPPA, 1998)</td>
<td>Age 12 or less. Problem: 13 is an adult? Not enforced.</td>
<td></td>
</tr>
<tr>
<td>FERPA</td>
<td>Doesn’t stop runaway data collection, or surveillance outsourcing to corporations</td>
<td></td>
</tr>
<tr>
<td>Drivers Privacy Protection Act (DPPA)</td>
<td>So why do many states still sell your data?</td>
<td></td>
</tr>
<tr>
<td>Privacy Act of 1974 (Govt data collection)</td>
<td>Gutted by exceptions and outsourcing to corporations</td>
<td></td>
</tr>
<tr>
<td>Right to Financial Privacy Act 1978 (Govt data collection)</td>
<td>Gutted by Patriot Act</td>
<td></td>
</tr>
<tr>
<td>FOIA (data review)</td>
<td>Agencies can slow-walk it</td>
<td></td>
</tr>
<tr>
<td>Patriot Act (I and II), Freedom Act, FISA (I and II), 215, 702, 12333 ...</td>
<td>It’s unclear gov’t follows laws</td>
<td></td>
</tr>
<tr>
<td>FISA Court (surveillance)</td>
<td>Often hears 1 side, limited investigative ability, mainly secret, a rubber stamp</td>
<td></td>
</tr>
<tr>
<td>State Laws</td>
<td>They vary and can’t solve a national issue.</td>
<td></td>
</tr>
<tr>
<td>Problem: Few to no regulations</td>
<td>Online data collection, social media, data selling, data aggregation, AI processing, profile compilations, data security &amp; encryption for PI, etc</td>
<td></td>
</tr>
</tbody>
</table>
The Internet: “Surveillance is its Business Model”

– Bruce Schneier

- Web searches
- Web surfing behavior:
  - Pages visited
  - Every click you make
- Posts:
  - Social media
  - Blogs
  - Websites
  - Forums
- Contact lists
- Purchasing behavior and history
- Email, texts, tweets, chats, IMs, VOIP ...
- ISPs can read your connection and sell your data (Deep Packet Inspection)
- Meta Pixel and Google reCAPTCHA

Loss of privacy is huge!

Goal: know you *intimately*

Tracking You: 3 Hours Online

Each circle is an event.
Each dot is a tracker for that event.


See all trackers on a website –
https://themarkup.org/blacklight
Use VPNs for Privacy (or TOR)

Look for:
- Trust
- No logging
- Speed

- Free Browser
- NoScript, HTTPS Everywhere
- Reduces trackers, defends identity
- Requires Expertise
- Not anonymous from a “ubiquitous surveillor”

Read:  
www.torproject.org/  
www.forbes.com/advisor/in/business/software/are-vpns-safe/  
www.pcmag.com/how-to/what-is-a-vpn-and-why-you-need-one
What Do They Know About You?

Google Example:

– Every place you search in Google Maps
– Every question you ask Google Assistant
– Every comment you leave on YouTube
– Every video you watch
– Every news article you read on Google News
– Every ad you view or visit in Google’s products
– Every app you open, search for, download
– Every gmail

... and more

From: “How to Download a Copy of Everything Google Knows About You”
– Todd Haselton, 3/30/18, CNBC.com
What Do They Know About You?

Why not download your raw data and find out?

Google

https://support.google.com/accounts/answer/3024190?hl=en

Facebook

https://www.facebook.com/help/212802592074644

Amazon

Go to “My Account”, then “Request My Data”

Much more intimate than any diary!
Emails & Texts Could Expose Your Life

Emails:

- Most use encrypted communications
- But the emails are **not** encrypted
- They can be read when not in transit

What You Can Do:

1. Use “end-to-end” (E2EE) encryption (S/MIME, PGP)
2. Trick: use encrypted attachments

**Solution:** Vendors agree on “end-to-end” encryption standard for product interoperability

**Texts**

- No Encryption – SMS
- Must Enable – Telegram
- E2EE by Default – Signal, iMessage, Messenger, Instagram, WhatsApp (since 12/23)

Read - [www.pcmag.com/picks/the-best-email-encryption-services](http://www.pcmag.com/picks/the-best-email-encryption-services)
[www.ionos.com/digitalguide/e-mail/e-mail-security/email-encryption-with-ssl/](http://www.ionos.com/digitalguide/e-mail/e-mail-security/email-encryption-with-ssl/)
[https://windowsreport.com/how-to-send-secure-email-outlook/](https://windowsreport.com/how-to-send-secure-email-outlook/)
## How To Stop Their Tracking

<table>
<thead>
<tr>
<th>Mechanism:</th>
<th>To Defeat It:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location Tracking</td>
<td>Use a burner cell w/o apps. Avoid FR, wearables, new cars, bank cards (pay cash)</td>
</tr>
<tr>
<td>Login Tracking (to Google, Chrome, Gmail, Facebook, Disqus, Yahoo, Microsoft...)</td>
<td>Don’t log in. Delete cookies/cache on shutdown</td>
</tr>
<tr>
<td>Communications (Email, texts, tweets, IM’s)</td>
<td>End-to-end Encryption (E2EE)</td>
</tr>
<tr>
<td>ISP Monitoring (DPI)</td>
<td>Virtual Private Network, HTTPS, TOR</td>
</tr>
<tr>
<td>Web bugs, cookies, flash cookies, 3rd party cookies, evercookies, email trackers ...</td>
<td>Browser settings and extensions, clear cache, Email forwarding/protectors</td>
</tr>
<tr>
<td>Spy Browsers (eg Chrome)</td>
<td>Use another browser</td>
</tr>
<tr>
<td>Spy Browser Extensions</td>
<td>Don’t install</td>
</tr>
<tr>
<td>Spy OS’s (eg, Chrome OS, Windows 10)</td>
<td>Use Linux (Windows → change defaults)</td>
</tr>
<tr>
<td>Spy Apps</td>
<td>Don’t install. Install anti-malware</td>
</tr>
<tr>
<td>Mac and IP addresses</td>
<td>Change or Mask or TOR</td>
</tr>
<tr>
<td>Device Fingerprinting</td>
<td>Browser settings and extensions</td>
</tr>
<tr>
<td>Internet Search history</td>
<td>Use DuckDuckGo or StartPage</td>
</tr>
<tr>
<td>Cracking your Password</td>
<td>2 Factor Authentication (2FA), Password Mgr, verify password complexity</td>
</tr>
<tr>
<td>Credit / Debit card tracking</td>
<td>Use cash or virtual credit cards.</td>
</tr>
</tbody>
</table>

---

**Requires Expertise & Time.**  
**Solution:** a Privacy Right and Laws

---

Read: [https://pixelprivacy.com/resources/](https://pixelprivacy.com/resources/)
Device Fingerprinting

How to Identify & Track People Without them Knowing
(circumvents VPNs, no cookies, etc)

By Dr. Ting Fang Yen @ DataVisor.com

Browser vs. Mobile App

HTTP cookie, OS version, Browser version, Browser configuration, IP address, ...
Device ID, Biometrics, Smartphone sensors (GPS, gyroscope, accelerometers, ...), WiFi networks, ...

Identifiers used in device fingerprinting: browser vs. mobile app. Compared to web services, mobile apps reside on the device and hence have access to more fine-grained information for device fingerprinting.

567,000 Fingerprints

From the Medium article cited below

How to Identify & Track People Without them Knowing (circumvents VPNs, no cookies, etc)

Another Technique: Secret Biometrics Collection

Test Your Browser: panopticlick.eff.org/ https://ipleak.net/ www.perfect-privacy.com
medium.com/slido-dev-blog/we-collected-500-000-browser-fingerprints-here-is-what-we-found-82c319464dc9
“Shadow Profiles”

How to Build Profiles Without People Knowing

Circumvents:

- Those who don’t sign up / login (eg FB, Google...)
- Informed consent
- Subjects’ control of their data
- Privacy laws

Read: www.howtogeek.com/768652/what-are-facebook-shadow-profiles-and-should-you-be-worried/
www.makeuseof.com/tag/facebook-shadow-profiles/
The Secret Life of Your iPhone

- Phone busy all night exfiltrating your data
- 5,400 data trackers active in a week

From “It’s the Middle of the Night. Do You Know Who Your iPhone is Talking To?”
Washington Post, by Geoffrey Fowler, 5/28/19
Apps & Browser Extensions Steal Your Privacy

ICSI study ==> 1,300 Android apps harvest data without permission!
NC State ==> Found 3,800 malware extensions affecting 60 M users in Chrome Store
Lockdown Privacy ==> Apple’s “Ask App Not to Track” does not work (9/21)

“Privacy Dashboard” for Android Apps

Installing Browser Extension

It’s a sham to place this privacy burden on users!

NC State study - www.washingtonpost.com/technology/2019/07/18/i-found-your-data-its-sale/?utm_term=.783750b9a51e
www.imore.com/these-apps-are-stealing-your-most-private-data-and-it-should-be-crime
www.rd.com/article/smartphone-apps-stealing-data/
www.washingtonpost.com/technology/2021/01/29/apple-privacy-nutrition-label/
www.washingtonpost.com/technology/2021/01/29/apple-privacy-nutrition-label/
The “Data Brokering” Industry

$230 billion business

- Unregulated
- Sell sensitive data without regard to harm!
  - Police officers
  - Rape victims
  - AIDS sufferers
  - Addled Seniors
  - Children
  - Political opponents
  - Your politics, race, religion, opinions...
  - To foreign powers
- Govt buys data to circumvent privacy laws!
- Categorizes people and imposes decisions on them

Solution: Obligations for PI vendors, rights for subjects, with effective penalties for violators

See: GDPR, FTC report: “A Call for Transparency & Accountability”
The Bogus “Consent” Industry

1. Worthless “consent” for installing Apps, Extensions...

2. “Privacy Policy”
   ... We reserve the right to change this policy at any time by posting the amended version on our website...
   Look for “change” or “alter” or “update”

3. Sign under Duress
   (1) Oligopoly – you have no choice
   (2) Time-pressure signings

4. “Dark Patterns”
   Designed to fool you!

Solutions: (1) Opt-out should be default
(2) Consumer Protection laws
Remove burden from Consumer put it on Corporations

The “Software Tools” Scandal

Collects your private data from:

- Medical (Hospitals, Pharmacies)
- Kids (schools, college applications)
- Finance (Banks, Mutual Funds)
- Tax prep companies
- Gov’t agencies
- Suicide hotlines
- more

May Collect:

- Screen contents (inc. PI & passwords)
- Device fingerprint
- User behavior
- Data used for undisclosed purposes
  (CNIL – French Privacy Commission)

HUGE Privacy violations

- Forces users to give Google data
- Penalizes users who want privacy (VPN users & those w/o Google Login)

Logos courtesy: Meta and Google
Data Breach

An organization appropriates your PI, then loses it

You pay the price!

Over 13 billion records lost since 2005 – hf est.

Solutions –
- If you store PI, you must:
  - Know what data you have
  - and where it is!
  - Encrypt the data
  - Logging
  - Meet security standards
  - Only collect necessary data
  - Delete old data
- Limits on cross-use, data selling
- Subjects’ rights
- Penalties for violators
- Default encryption for Windows
- Better MS password schemes
- Encrypted email, text, voip

Courtesy: csoonline.com

Annual number of data compromises and individuals impacted in the United States from 2005 to 2022

Courtesy: MediaFeed.org

Biggest DATA BREACHES of the 21st century

Marriott: 500m
Equifax: 143m
Adult Friend Finder: 412.2m
Anthem: 78.8m
eBay: 145m
JP Morgan Chase: 76m
Home Depot: 56m
Yahoo: 3b
Target Stores: 110m
Adobe: 38m
US Office of Personnel Management (OPM): 22m
Sony’s PlayStation Network: 77m
RSA Security: 40m
Heartland Payment Systems: 134m
TJX Companies, Inc: 94m

Courtesy: csoonline.com
Equifax Lost PI of 147 Million

So we can verify if your data was hacked, please provide:

Your Name: ___________________
SSN: ________________________

Equifax sees the breach as an opportunity for:
– Data collection
– Marketing
– CEO golden parachute of $18.4 million

Solutions:
– Inventory, Security, Encryption, Logging for PI
– Opt Out should be Default
– Change incentives
– Court relief for consumers (not arbitration)

Read: www.csoonline.com/article/567833/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html
https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement
Identity Theft

Identity Theft & Financial Fraud Cases Yearly

Source: FTC by way of https://identitytheft.org/statistics/

Corporations are fault, but ID theft costs YOU:

- Time (30 hrs avg)
- Money
- Emotional impact
- Credit effects on Jobs, Housing, Benefits
- etc

Common Types of Identity Theft

Credit Card Fraud: 133,015 reports
Employment or tax-related fraud: 82,051 reports
Phone or utilities fraud: 55,045 reports
Bank fraud: 50,517 reports
Loan or lease fraud: 30,034 reports
Government documents or benefits fraud: 25,849 reports

**Biometrics**

- Face
- DNA
- Fingerprint
- Voiceprint
- Iris
- Race
- Gender
- Word Choice
- Signature
- Dental
- Writing Style
- Handwriting
- Height/Wgt
- Gate
- Keystroking
- Retina
- Hair
- Ethnicity
- Eye color

Companies & Govt’s **really** want your biometrics!

A.I.

Stealing biometrics is fun!

---

**US Biometrics Market Growth**

CAGR 20%

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Value</td>
<td>3.52</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Face, Hand geometry, Voice, Signature, Iris, AFIS, Non-AFIS, Others

Courtesy: Global Market Insights @ gminsights.com

---


www.BiometricUpdate.com

© H. Fosdick
Anonymity?

“There’s No Such Thing as Anonymous Data” – HBR

You can be anonymous on the internet. Not against a ubiquitous surveillor.
School Panopticon Training Digital Peons

- Without consent
- Cameras everywhere (> 90% of HS & MS)
- Facial recognition soon
- Complete monitoring & data collection
  - Social Media
  - Chromebook, G Suite
  - Judge all they type
  - Confiscate student IP?
    - presumption of guilt
  - College
- Companies get student data
- Police integration
- FERPA & COPPA are ineffective

We have outsourced 24 x 7 data collection on our kids to private companies

- Our kids never type a private thought
- Will this data follow them for their entire lives?

Solution: National standards for Ed Tech Privacy.
Federal Licensing? Educational Consortia Builds Tools?

Read: www.theguardian.com/world/2019/oct/22/school-student-surveillance-bark-gaggle
www.eff.org/deeplinks/2020/02/schools-are-pushing-boundaries-surveillance-technologies

Vista Equity Partners – predictive modeling
Your Shopping Experience

- Bluetooth tracking
- Facial Recognition (some stores)

May collect –
- PI
- Card & Bank Act Numbers
- Financial
- Health info
- Device fingerprint
- Demographics
- Behavioral analysis
- Purchase history
- Location

1,400 buyers
84.51 (data broker)
Kroger Personal Finance
Kroger Precision Mkting

Meta, Google,
Bing, Pinterest,
Snapchat

https://themarkup.org/privacy/2023/02/16/forget-milk-and-eggs-supermarkets-are-having-a-fire-sale-on-data-about-you
Employer Surveillance

In most states, anything goes...

Problem: Our Work and Private lives overlap

How?
- Software monitoring
- Internet usage
- Keylogging
- Email
- Phone & voicemail
- Video
- Location
- Badges
- Social media
- Blogs / forums

Studies show a little monitoring is beneficial, too much is counterproductive

Your Car is a Privacy Nightmare!

What has four wheels, collects your sexual activity data and sells your personal information?

Probably your car.

25 car brands tested
25 car brands failed

*Privacy Not Included

– Car is a computer you sit in
– Reports to it’s “real owner”
– Cameras watch you & the road
– Audio too
– “Consent” is buying the car … or just riding in it!
– You can’t access “your” data
– And your data is not encrypted and hacked!  (VW, Toyota, M-Benz...)

Includes biometrics, health data, sexual activity & orientation, conversations, visuals, driving behavior, location tracking . . .

“Vehicle Data Hubs” collate and sell your info


Wearables -> Let’s Monitor Your Body!

- No HIPAA protections!
- Who gets the data?
- Security?
- Kept for how long?
- Future Use?

Kids are tracked too

Once you give your data out ...


Let’s Monitor You at Home!

Voice assistants, TVs, toys, doorbell, vacuums, cells, computers, lights, thermostats, gas & electric meters, Nest, appliances (refrig, microwave, washer, dryer, more), baby monitors, gameboxes, wearables, and more!

Nest Cam Indoor security camera
Plug-in-and-go security.

The Nest Cam Indoor security camera is designed to help you look after your home and family – even when you’re away.

BUY NOW

Courtesy: Amazon.com

Photo: James Pace-cornsilo/Washington Post
Eye: EvolutionaryNews.org

Courtesy: engadget.com, ear: singularityhub.com

Courtesy: TheStar.com

Courtesy: Amazon.com

Courtesy: NakedSecurity.sophos.com

Courtesy: SingularityHub

Courtesy: Motorola

Courtesy: NakedSecurity.sophos.com

Courtesy: Amazon.com

Photo: James Pace-cornsilo/Washington Post
Eye: EvolutionaryNews.org

 Courtesy: Amazon.com

TV
Internet of Things (IoT)

+ Features & Convenience

- Every device a monitor
- Sensors everywhere (video, audio ...)
- Invading your home (appliances)
- Invading you (wearables)

Solutions:

Privacy needs a Trust Mark too!
Also Opt-out & ability to turn off web connect

"Internet Pollution" term coined by H. Fosdick

US Cyber Trust Mark

Read: www.insiderintelligence.com/insights/ot-security-privacy/
https://link.springer.com/chapter/10.1007/978-3-030-82786-1_11

© H. Fosdick
Hacking IoT: from Fish Tank to Casino

IoT = Security & Privacy Nightmare

TikTok – a red herring

- China can buy any data...
  - Acxiom
  - Experian
  - Corelogic
  - Epsilon
  - Equifax
  - others

- Or sell us devices...
  - Huawei routers etc
  - Drones
  - Chips, Computer hardware
  - Cell phones (7 of 10 come from China)

- Or just steal it...
  - Equifax 145m
  - US Office Pers Mgmt 2m
  - Anthem 78m
  - Marriott 500m

Solutions: (1) regulate data broker industry
(2) security standards for PI
Sweden – Cashless Society

Pay by (1) Mobile App or (2) Card

- Tracks ALL transactions
- No privacy
- No more underground economy
- No more tax evasion
- Saves / makes companies money

The ultimate corporate / government dream!

FedNow – Will US resist?

Your Life-long Personal Database

The "Digital You"
- in databases
- in communications
- behavioral profiles

How will this data be used against you in future?

(Only credit data ages out by federal law)

"I used to be free!"

Are you free in a society with surveillance and forever data?

Courtesy: Bibliotecha Alexandrina via Bibalex.org

Read:
III. Gov’t Surveillance
I support our gov’t employees
(DHS, NSA, FBI, TSA, CIA, police ...)

My criticisms are not of them!

--> What I’m talking about are policies

Cautions :
- Secrecy !
- Programs are disguised
- Confusion is intentional
National Security vs Personal Security

Security of the Nation vs Security of 330 million individuals

- Gov’t fights encryption (cells, emails, texts, etc)
- NSA keeps backdoors & zero-days secret
- FBI seizes data w/o warrant (NSLs, gag orders)
- Mass search & surveillance
- Stolen NSA tools used against us (WannyCry, EternalBlue...)
- No due process for:
  - Blacklists
  - NSL’s & gag orders
  - Civil asset forfeiture

Do such policies make you more secure?

“The NSA is willing to compromise the security of everything to get what they want”

- Schneier

Mass Search is Unconstitutional

US Constitution – 4th Amendment –

“The right of the people to be secure in their persons, houses, papers, and effects ... shall not be violated ... but upon probable cause ... describing the place to be searched, and the persons or things to be seized.”

“General Warrants” are unconstitutional

“Washington is violating the privacy rights guaranteed to us by the 4th Amendment.”
Data Mining All Your Communications

Surveillance programs include:

Xkeyscore, Prism, Boundless Informant, Mystic, Carnivore, Bullrun, FAA702 Upstream, Muscular, Turbine, Quantumhand, Fairview, Stormbrew, Blarney, Oakstar .

Read: www.wired.com/2015/03/data-and-goliath-nsa-metadata-spying-your-secrets/ eff.org aclu.org epic.org pogo.org
www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/5
Charlie Savage’s Power Wars, aclu.org/files/pdfs/eavesdropping101.pdf
www.pbs.org/newshour/show/nsa-collects-word-for-word-every-domestic-communication#transcript
"If the history of these surveillance programs teaches us anything, it’s that the government can subvert seemingly clear legal standards ... to accommodate its desire [for] ... surveillance...”

– Jake Laperruque
FISA Court

A Secret Court that makes secret law

- 1 judge decides
- Hears only govt’s side
- Can’t investigate govt claims
- Rejects 0.03% of govt requests

This is how we gutted the 4th Amendment

USA Freedom Act (2015)

- Court to send changes in law to Congress
- May hear other side
- Minimal investigative ability
- Doesn’t stop mass surveillance

Read: www.eff.org/issues/privacy
www.aclu.org/issues/privacy-technology
https://epic.org/

Courtesy: epic.org
*Methodology for counting applications, modifications and denials
Mass Surveillance Doesn’t Work

Example:
Phone Call Metadata

Effective at destroying your privacy (Principle of “Big Data”)

“With enough metadata we don’t need content” – Michael Hayden

Not Effective at finding terrorists!

Pres. Obama: “50 terrorist plots foiled” → Turned out to be one ... a donation!

Privacy & Civil Liberties Oversight Board (2014)
Charlie Savage (2015)

→ “Not essential in preventing attacks”
→ Not one terrorist found
→ FBI calls NSA tips worthless
Why Failure? The “Percentage Fallacy”

- 99% accuracy
- Assume 1 of 100,000 is a terrorist
- Nationwide 3,230 terrorists
- Misses 32 terrorists (false negatives)
- Identifies 3.23 million false positives

The 3,198 terrorists are hidden in the 3.23 million false positives!

For mass surveillance, 99% accuracy is not enough
Surveillance Erodes Freedom

On PBS

Chilling Effect or Self-Censorship

on freedom of speech, press, religion, assembly

Democracy Requires Privacy

Impeachment indictment:

1. Violated opponent’s privacy (the Democratic party)
2. Inappropriate data cross use (hassled opponents w/ IRS)

“Trust Us” doesn’t work.

That’s why we have:

- Constitution
- Bill of Rights
- Division of powers between 3 branches
- Checks & balances
- Congressional oversight
- Judicial review

...
Democracy Requires Privacy

The guy Presidents couldn’t fire ...

- He blackmailed Presidents & Congress
- Conducted illegal actions against political opponents (COINTELPRO)
- Tried to get Dr. King to kill himself

---

We need security agencies! But “Trust Us” doesn’t work.

Coutesy: the Daily Beast reference below

IV. Solutions

Technology can assist, but the solutions are political
We Are “Digital Peons”

- Your entire life is digitized
- You can not live a modern existence otherwise
- Your data is appropriated
- You don’t know how, when or where your personal data is used – or sold
- You can’t review accuracy
- You have no assurance it is secured

Decisions critically affecting your life are made based on “Secret Data” ... and secret AI-based algorithms.
Your "Digital Doppelganger" Determines Your Life!

The Real You

The Digital You

And you don’t even know him!
Solution: A “Privacy Architecture”

- Spotty Privacy Laws
- Little Judicial protection
- We violate our Bill of Rights

- EU and national laws
  - General Data Protection Regulation (GDPR)

- US Bill of Rights
- Euro Convention on Human Rights
- Euro Charter of Fundamental Rights

- UN Universal Declaration of Human Rights

Courtesy: Forrester Research sourced from ZDNet.com
General Data Protection Regulation (GDPR)

Processor Obligations:

- Limited cross-use
- Security, encryption, logging standards for PI
- Actual penalties!
- Limit data gathered plus time constraints
- Must disclose data collection
- Anonymize data
- Keep processing records
- Compliance Officer
- Notify of data breach

Subject Rights:

- Default is Opt-Out
- Requires Informed Consent
- Can withdraw it
- Can review his data
- Can correct data
- Can be forgotten (erase data)
- Can transfer data

© H. Fosdick
Cal. Consumer Privacy Act (CCPA)

(CCPA 2018 amended by CPRA 2020, Delete Act 2023)

Consumers can
+ See their data
+ Delete their data
+ Stop data sales
+ Opt-out

– Only applies to large companies
– Only applies to collected data (not bought)
– Default is still Opt-in
– Excludes HIPAA, FCRA, GLB data
– Limited ability to stop cross-use
– No consumer lawsuits

washingtonpost.com/technology/2020/02/06/ccpa-faq/    en.wikipedia.org/wiki/California_Privacy_Rights_Act
<table>
<thead>
<tr>
<th>GDPR</th>
<th>CCPA</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Scope</strong></td>
<td></td>
</tr>
<tr>
<td>&quot;Personal data&quot; is any information relating to or that can be used to identify a specific person. It does not include the &quot;household&quot; stipulation.</td>
<td>&quot;Personal information&quot; is anything that identifies, relates to, describes, is capable of being associated with, or could be reasonably linked to a particular person or household.</td>
</tr>
<tr>
<td><strong>Covered Entities</strong></td>
<td></td>
</tr>
<tr>
<td>You don’t technically need to be a &quot;business&quot; at all - you just need to control or process relevant information.</td>
<td>The CCPA defines a &quot;business&quot; as a for-profit legal entity or sole proprietorship.</td>
</tr>
<tr>
<td><strong>Disclosure / Transparency Obligations</strong></td>
<td></td>
</tr>
<tr>
<td>An entity is required to provide the identity and the contact details of the data controller, the recipients of that data, the legal basis and purposes for processing, the retention period, the right of access and more.</td>
<td>Under the CCPA, businesses need to inform consumers at or before the point of collection what information is being collected and why it’s necessary.</td>
</tr>
<tr>
<td><strong>Right of Access</strong></td>
<td></td>
</tr>
<tr>
<td>The GDPR ALSO allows people to learn how long that information is being retained. The GDPR also has an additional &quot;right to portability&quot; in certain cases.</td>
<td>Both the GDPR and the CCPA give consumers the right to not only learn what information is being collected, but to also get a complete copy of that information.</td>
</tr>
<tr>
<td><strong>Right to Deletion</strong></td>
<td></td>
</tr>
<tr>
<td>The GDPR applies to ALL data concerning a data subject, no matter where it came from.</td>
<td>The CCPA, however, only applies to data collected FROM the consumer.</td>
</tr>
<tr>
<td><strong>Right to Opt-Out</strong></td>
<td></td>
</tr>
<tr>
<td>The GDPR, however, includes no such right. However, the GDPR is so strict in other areas that if a consumer didn’t want you to store and sell their data, there are other techniques they could use.</td>
<td>At any moment, the CCPA allows people to opt out of a business’ ability to collect or sell their personal data. At that point, a business is prohibited from doing anything meaningful with that data in any way.</td>
</tr>
</tbody>
</table>

GDPR is better ... but it has an enforcement problem
Solutions – Corporate

- Need a fundamental right to privacy
- Shift privacy burden to data holders from individuals
- Stop Fake Consent
  - Opt Out should be the default
  - Require Informed Consent
  - Fix consent under duress or w/o real choice
  - Eliminate bogus “Privacy” Policies
- Any entity holding PI must abide by certain rules:
  - Data inventory
  - Security standards
  - Logging
  - Encryption for PI
  - Cross-use restrictions
  - 2FA sb available everywhere
  - Sales restrictions
  - Subject’s rights (assent, review, correct…)
  - No data appropriation
  - 0-knowledge keys & authentication
  - Disclose how algorithms use PI
- Data broker regulation
- Effective penalties for violators
- Require encryption for consumer devices by default
- Security & Privacy must be made priorities for coders
- Deny mergers and enforce Anti-trust!
- Outsourcing and long contacter chains should NOT allow denial of responsibility
- You collect the data, you’re responsible for it!

- 3 Keys –
  - Opt-out as default
  - No data Cross-use
  - Data security/privacy stds

Read: GDPR, White House report: “Consumer Privacy Bill of Rights”
Solutions – Government

Fear drove our laws after 9/11. Time for a course correction.

- Adhere to the US Constitution
  - Stop domestic mass search & surveillance
- Oversight required for Top Secret America
  - Congress
  - Judiciary
- No NSLs, gag orders – these need a judge and warrant!
- Executive Orders are not sufficient for mass search
- Need real Judicial Oversight
  - Fix or eliminate FISA court
  - Needs both sides represented effectively
  - Needs true investigative abilities
  - Needs to verify its legal interpretations are followed
  - Needs to report to Congressional committee
  - Fix judge selection & single-judge rulings
  - Still a secret court making secret law -> bad
- Balance national security and personal security
  - Encryption for email, texting, cell phones
  - Stop weakening security for backdoors & zero-days
  - Stolen NSA tools used against us
  - No SSN for purchases over $10,000
  - National BIPA for biometrics
- Fix PCLOB (Privacy Civil Liberties Oversight Board)
- Need Privacy Czar or Agency or “CFPB” board

- Transparent rules required
  - That’s how democracy works
- Due process required
  - Blacklists
  - Borders
  - Civil asset forfeiture
  - Within 100 miles of the border
  - “Open Fields” doctrine
- Regulate Govt data access
  - Govt should declare what data it has or uses on Citizens
  - Ensure agencies don’t read novel meanings into laws
  - No buying or trading for data you’re can’t collect!
  - No trading with GCHQ / 5-Eyes for info on US citizens
  - Rules for data cross-use between agencies
  - Fix over-classification

“Privacy” Legislation?

We Want:
+ Privacy
+ Control
+ Personal Security
+ Accountability for Harm

Corporations & Gov’t Want:
- Status quo (with tweaks)
- Override state privacy laws
- Restrictions they can circumvent
  1. Opt-out as default
  2. Bogus consent
  3. Data cross-use

“The preferences of the average American have a near-zero... effect on public policy.”
- Gilens & Page study
→ State privacy laws have proven this true.

Likely outcome → a Fake “Privacy” Law

“FAKE”

Images: People: interregmr.eu, Fake stamp: DreamsTime.com
Time to Update the Fairy Tale . . .

Questions ?
V. Extra Slides

Good info that didn’t fit
Your TV Monitors You

- Opt-in is default
- ACR takes 7,200 images per hour of what you watch (2/sec)
- Your data is correlated and sold

What You Can Do:
- Change settings to Opt-out
- Avoid using TV as internet browser
- Secure your router
- Scandals & Hacking ==> FBI warning

Read: theguardian.com/technology/2022/jan/29/what-your-smart-tv-knows-about-you-and-how-to-stop-it-harvesting-data  
patch.com/us/across-america/smart-tvs-may-be-watching-listening-your-home-fbi-warns  
theregister.co.uk/2019/10/01/your_smart_tv_is_watching_you_says_princeton_privacy_prof/  
washingtonpost.com/technology/2019/09/18/you-watch-tv-your-tv-watches-back/
Employability Score from:
- Mannerisms
- Word choice
- Speaking voice
- Facial movement (some products)

Everything except what you actually say!

The Recruiter’s View:

- Bogus tool?
- Bogus Consent
- Will this be stored and used in future?

www.shrm.org/resourcesandtools/hr-topics/talent-acquisition/pages/hirevue-discontinues-facial-analysis-screening.aspx
Your Employer Sells Your Salary

IRS → Your Employer → Your PI → 147 million Record Data Breach

The Work Number from Equifax

Your salary & work history for sale

190 million employees

... and the company collecting it lost it in a data breach!

Read: nbcnews.com/technolog/exclusive-your-employer-may-share-your-salary-equifax-might-sell-1B8173066
Powerful Digital Monopolies

Google
- Several Hundred Companies!
  - DoubleClick
  - Youtube
  - Ad
  - Competitors
  - Motorola
  - Mobility
  - Waze
  - Nest

Alphabet
- Over 100 Companies!
  - Alexa
  - Convergence
  - Ring
  - Blink
  - DeepMind
  - Whole Foods
  - iRobot
  - Roomba
  - Zappos
  - Egghead
  - Software
  - Haven
  - Healthcare

Meta
- Over 80 Companies!
  - Facebook
  - Instagram
  - WhatsApp
  - Lightbox
  - Drop.io
  - ConnectU
  - Oculus VR
  - Social Media
  - Competitors

Amazon
- Over 80 Companies!
  - PillPack
  - Haven
  - Healthcare

Results:
- Control of your PI
- Political power

Solution:
Deny mergers, buyouts
Enforce anti-trust!
Those Who Seize Your Privacy Know Its Value!

"If you have something that you don’t want anyone to know, maybe you shouldn’t be doing it in the first place.”

– Eric Schmidt, ex-Google

– Deletes google accounts critical of him
– Tried to delete record of his political donations
– Sicked his lawyers on mistress who posted about him

“Think he knows?”

“You have to fight for your privacy or you will lose it”

Eric Schmidt, Google Chairman, 25 May 2013

Who Loses Privacy?

Those who lack:
- Expertise
- Time
- Money

The old, the young, the poor, the uneducated, the vulnerable

Meta / Facebook

Google

Cell apps

Opt-in defaults

IoT

Internet tracking

Privacy

Email

More!
3 States of Surveillance

No Surveillance

+ Freedom

– But a country needs to protect itself!

Surveillance

+ Necessary to protect country!

– Chilling Effect
– Self-censorship
– Permanent records
– Data cross use
– Data breaches
– No data rights

Surveillance + Secret Action

– No Citizen rights
– Penalties applied w/o trial
– Police state

?
China’s “Social Credit”

Purpose: Use technology to shape behavior

Score based on:
- Whatever the government wants

Consequences:
- Jobs, loans, housing
- Travel bans
- School admissions
- Public shaming
- Fines
- Minority persecution

Are we sleep-walking into a similar system ruled by corporate “little brothers”?

Read: businessinsider.com/china-social-credit-system-punishments-and-rewards-explained-2018-4?op=1
Why US Gov’t Secrecy?

National Security leaders believe:

- They’ll get blamed if anything bad happens
  (Loss of life is quantifiable, loss of privacy is not)
- Secrecy means efficacy
- They don’t get that “Trust Us” is inimical to democracy
- Congress rejected Total Information Awareness in 2003
- Thus they believe Courts, Congress, or Public would stop these programs if they knew

How They Maintain Secrecy:

- Threat inflation
- Renaming programs
- Overlapping programs
- Misinterpreting laws
- Wordsmithing
- Misleading statements
- Lie, then quietly retract it

“Trust Us” doesn’t work!

That’s why we have Bill of Rights, distribution of powers, 3 branches of gov’t, checks and balances, congressional oversight, judicial review, etc.
The National Security State

“No nation could preserve its freedom in the midst of continual warfare”
– James Madison

Panopticon

Militarization of Policing  Huge DHS  Mass Digital Surveillance  School, Public Surveillance  Surveillance Capitalism  Top Secret America

Reasons for 9/11 misrepresented  4th Amendment subverted, Security laws misinterpreted

Continuous War Since 1991

(Assuming you consider the 1990s Iraqi embargo an act of war, as did the UN)

Our Wars

Afghanistan  2001 - 2022
Mideast Armed Operations (Pakistan, Yemen, Iran, Saudi Arabia, Philippines, Iraq, Syria, others)  2001 - ?
Iraq and Syria Armed Operations against ISIS  2014 - ?
African Armed Operations (Liberia, Cameroon, Uganda, Sudan, Ethiopia, Djibouti, Mali, Tunisia, Kenya, Niger, Somalia, others)  2014 - ?
Iraq War II and armed occupation  2003 – 2011
Libya  2011, 2016
Iraqi No-Fly Zones and Embargo enforcement  1991 – 2003

Kosovo  1999
Haiti  1994 - 1995
Bosnia  1992 – 1995
Iraq War I (Gulf War)  1990 – 1991
Panama  1989 - 1990

Osama Bin Laden Explains Why He Attacked US on 9/11:
V. Questions