The Surreptitious Assault on Privacy, Security, and Freedom

Mike Gerwitz

26 March, LibrePlanet 2017

N.B.: These slides appear as they were presented at LibrePlanet 2017 (with the exception of this slide).

For up-to-date slides, see:
https://mikegerwitz.com/talks/sapsf

For the source code to this presentation, see:
https://mikegerwitz.com/projects/sapsf

You're Being Tracked.

You're Being Tracked.

(No, really, I have references.)

- Most people carry mobile phones
- Synonymous with individual

- Most people carry mobile phones
- Synonymous with individual
- Excellent tracking devices

Fundamentally Needed

- Phone needs tower to make and receive calls
- Gives away approximate location [75]
- Multiple towers: signal delay; triangulate

[3]

Cell-Site Simulators

- IMSI-Catchers
- Masquerade as cell towers
- Most popular: Stingray

[30]

Cell-Site Simulators

- IMSI-Catchers
- Masquerade as cell towers
- Most popular: Stingray
- Free/libre Android program AIMSICD available on F-Droid attempts to detect [13]

[30]

TOP SECRET//SI//NOFORN

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

WASHINGTON, D.C.

IN RE APPLICATION OF THE
FEDERAL BUREAU OF INVESTIGATION
FOR AN ORDER REQUIRING THE
PRODUCTION OF TANGIBLE THINGS
FROM VERIZON BUSINESS NETWORK SERVICES,
INC. ON BEHALF OF MCI COMMUNICATION
SERVICES, INC. D/B/A VERIZON
BUSINESS SERVICES.

Docket Number: BR

13-80

SECONDARY ORDER

This Court having found that the Application of the Federal Bureau of

Senator Ron Wyden, 26 May 2011:

> *I have served on the Intelligence Committee for over a decade and I wish to deliver a warning this afternoon. When the American people find out how their government has secretly interpreted [the business records provision of FISA], they are going to be stunned and they are going to be angry.* [103]

Verizon Metadata

- June 2013—Guardian releases leaked document ordering Verizon to collect "telephony metadata" [43, 39]

  [. . .] (i) between the United States and abroad; or (ii) wholly within the United States, including local telephone calls. [116]

Verizon Metadata

- June 2013—Guardian releases leaked document ordering Verizon to collect "telephony metadata" [43, 39]

  [. . .] (i) between the United States and abroad; or (ii) wholly within the United States, including local telephone calls. [116]

- Routing information, source and destination telephone numbers, IMSI and IMEI numbers, and time and duration of the call [116, 78]

Verizon Metadata

- June 2013—Guardian releases leaked document ordering Verizon to collect "telephony metadata" [43, 39]

  [. . .] (i) between the United States and abroad; or (ii) wholly within the United States, including local telephone calls. *[116]*

- Routing information, source and destination telephone numbers, IMSI and IMEI numbers, and time and duration of the call [116, 78]
- "Business records" provision partly declassified by Clapper on 6 June 2013 [20]
- The American people were stunned and angry

Metadata Matters

[74]

- EFF on "Why Metadata Matters": [78]

Metadata Matters

[74]

- EFF on "Why Metadata Matters": [78]
  - They know you rang a phone sex service at 2:24 am and spoke for 18 minutes. But they don't know what you talked about.

Metadata Matters

[74]

- EFF on "Why Metadata Matters": [78]
  - They know you rang a phone sex service at 2:24 am and spoke for 18 minutes. But they don't know what you talked about.
  - They know you spoke with an HIV testing service, then your doctor, then your health insurance company in the same hour. But they don't know what was discussed.

ESSID and MAC Broadcast

- Device may broadcast ESSIDs of past hidden networks
- Expose unique hardware identifiers (MAC address)

ESSID and MAC Broadcast

- Device may broadcast ESSIDs of past hidden networks
- Expose unique hardware identifiers (MAC address)
- Defending against this is difficult

ESSID and MAC Broadcast

- Device may broadcast ESSIDs of past hidden networks
- Expose unique hardware identifiers (MAC address)
- Defending against this is difficult
  - *Turn off Wifi* in untrusted places
  - Turn off settings to auto-connect when receiving e.g. MMS

ESSID and MAC Broadcast

- Device may broadcast ESSIDs of past hidden networks
- Expose unique hardware identifiers (MAC address)
- Defending against this is difficult
  - *Turn off Wifi* in untrusted places
  - Turn off settings to auto-connect when receiving e.g. MMS
  - Use cellular data (e.g. {2,3,4}G)

ESSID and MAC Broadcast

- Device may broadcast ESSIDs of past hidden networks
- Expose unique hardware identifiers (MAC address)
- Defending against this is difficult
  - *Turn off Wifi* in untrusted places
  - Turn off settings to auto-connect when receiving e.g. MMS
  - Use cellular data (e.g. {2,3,4}G)
  - MAC address randomization works poorly [61]

Global Positioning System (GPS)


[29]

- Not inherently a surveillance tool

Global Positioning System (GPS)


[29]

- Not inherently a surveillance tool
- Often enabled, and programs abuse it [125]
  - Legitimate: navigation, social media, photos, nearby friends, finding lost phones, location-relative searches, etc.

Global Positioning System (GPS)


[29]

- Not inherently a surveillance tool
- Often enabled, and programs abuse it [125]
  - Legitimate: navigation, social media, photos, nearby friends, finding lost phones, location-relative searches, etc.
- If phone is compromised, location is known

But I Want GPS!

- Is the program transparent in what data it sends? (Is the source code available?) [125]
  - 2010: 47 of top 100 Android and iOS apps sent location to devs and third parties [120]
  - Ex: *Angry Birds* sent address book, location, and device ID to third party [16]
- Does the program let you disable those [anti-]features?

But I Want GPS!

- Is the program transparent in what data it sends? (Is the source code available?) [125]
  - 2010: 47 of top 100 Android and iOS apps sent location to devs and third parties [120]
  - Ex: *Angry Birds* sent address book, location, and device ID to third party [16]
- Does the program let you disable those [anti-]features?
- Pre-download location-sensitive data (e.g. street maps)
  - OsmAnd (free software, Android and iOS) [80]

Location Services

- No GPS? No problem!
- Mozilla Location Services, OpenMobileNetwork, . . . [66, 77]
- Wifi Positioning System; Bluetooth networks; nearby cell towers [123]
  - Signal strength and SSIDs and MACs of Access Points [108, 52, 55]

Location Services

- No GPS? No problem!
- Mozilla Location Services, OpenMobileNetwork, . . . [66, 77]
- Wifi Positioning System; Bluetooth networks; nearby cell towers [123]
  - Signal strength and SSIDs and MACs of Access Points [108, 52, 55]
- Some gathered by Google Street View cars
- Your device may report back nearby networks to build a more comprehensive database

Location Services

- No GPS? No problem!
- Mozilla Location Services, OpenMobileNetwork, . . . [66, 77]
- Wifi Positioning System; Bluetooth networks; nearby cell towers [123]
  - Signal strength and SSIDs and MACs of Access Points [108, 52, 55]
- Some gathered by Google Street View cars
- Your device may report back nearby networks to build a more comprehensive database
- Works even where GPS and Cell signals cannot penetrate
  - Can be *more* accurate than GPS (e.g. what store in a shopping mall)

Untrusted/Proprietary OS

- Who does your phone work for?
  - Apple? Google? Microsoft? Blackberry? Your manufacturer too?
- Carry everywhere you go, but fundamentally cannot trust it [84]

Untrusted/Proprietary OS

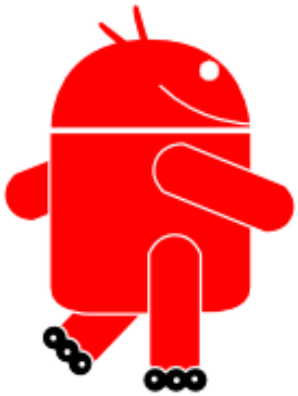
- Who does your phone work for?
  - Apple? Google? Microsoft? Blackberry? Your manufacturer too?
- Carry everywhere you go, but fundamentally cannot trust it [84]
- Some come with gratis surveillance
  - BLU phones sent SMS messages, contacts, call history, IMEIs, and more to third-party servers without users' knowledge or censent [54]

Free/Libre Mobile OS?

- Android is supposedly free software
  - But every phone requires proprietary drivers, or contains proprietary software

Free/Libre Mobile OS?

- Android is supposedly free software
  - But every phone requires proprietary drivers, or contains proprietary software
- Replicant [89]
  - Niche. Largely work of one developer now. (Help if you can!)



Replicant

Modem Isolation

- But modem still runs non-free software [88]
- Sometimes has access to CPU, disk, and memory [90]

What about your car?

- **Information about you and your accounts with us:** such as your name, address, telephone number, date of birth, e-mail address, login information, demographic data, gender, password, PIN, emergency contact information, information about the acquisition and financing of your vehicle, like whether or not you have financed or leased your vehicle, the lease/financing term, and billing information, like your credit card number, CVV code and expiration date.
- **Information about your vehicle:** such as license plate number, vehicle identification number (VIN), mileage, oil/battery status, fuel or charging history, electrical system function, gear status, and diagnostic trouble codes.
- **Information about the use of your vehicle, including operational and safety related information:** such as GPS location, speed, air bag deployments, crash avoidance alerts, impact data, safety system status, braking and swerving/cornering events, event data recorder (EDR) data, seat belt settings, vehicle direction (heading), camera image and sensor data, voice command information, stability control or anti-lock events, security/theft alerts, infotainment system usage, and WiFi data usage.
- **Information about your device and how you interact with our products and services, including apps and websites:** such as IP address, browser type, unique device identifier, cookie data, associated identifying and usage information from your mobile phone, laptop, or other device.

[83]

- Since 2011, retains all GPS and system data to sell to third parties

"We know everyone who breaks the law, we know when you're doing it. We have GPS in your car, so we know what you're doing. By the way, we don't supply that data to anyone." [26]

—Jim Farley, VP/Marketing and Sales, 2014

"If you've got nothing to hide, you've got nothing to fear." *[93, 100, 68]*

—Joeseph Gobbels, Nazi propaganda minister

"If you've got nothing to hide, you've got nothing to fear." [93, 100, 68]

—Joeseph Gobbels, Nazi propaganda minister

—Richard Graham, British MP

Private Cameras in Plain View; Tinderloin, SF

[8]

"The idea that you can sort of meet in a public place and quietly have a conversation that we're sort of accustomed to from spy movies, that is really not realistic anymore,"
—Nadia Kayyali, EFF [8]

Access to Data

- Data can be obtained with a warrant or subpoena

Access to Data

- Data can be obtained with a warrant or subpoena
- Data can be compromised

Access to Data

- Data can be obtained with a warrant or subpoena
- Data can be compromised
- Chilling effect

Access to Data

- Data can be obtained with a warrant or subpoena
- Data can be compromised
- Chilling effect
- If you own a surveillance system, be responsible and considerate
  - Best way to restrict data is to *avoid collecting it to begin with*

What if all those cameras—including private—were connected?

NYPD Domain Awareness System[86]

Although NYPD documents indicate that the system is specifically designed for anti-terrorism operations, any incidental data it collects "for a legitimate law enforcement or public safety purpose" by DAS can be utilized by the police department. [111]

Domain Awareness System

- Partnership between the NYPD and Microsoft at a cost of $230M in 2013 [33, 86]
  - Surveillance cameras, license plate readers, radiation detectors, 911 system, criminal records, ...
- $>$ 6,000 surveillance cameras, $\frac{2}{3}$ private businesses [33, 75]

Domain Awareness System

- Partnership between the NYPD and Microsoft at a cost of $230M in 2013 [33, 86]
  - Surveillance cameras, license plate readers, radiation detectors, 911 system, criminal records, ...
- $>$ 6,000 surveillance cameras, $\frac{2}{3}$ private businesses [33, 75]
- Database of over 16 million plates, every car going into Lower Manhatten [33, 75]

Domain Awareness System

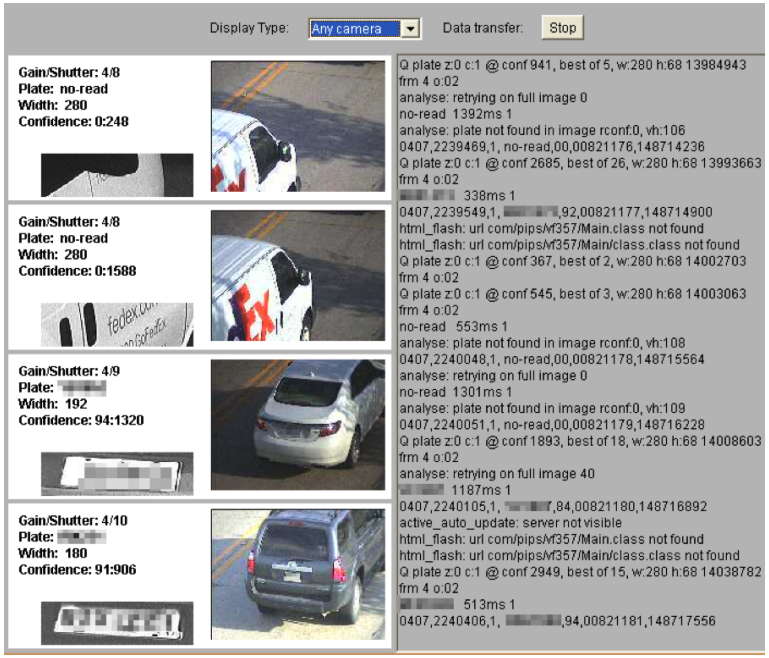
- Partnership between the NYPD and Microsoft at a cost of $230M in 2013 [33, 86]
  - Surveillance cameras, license plate readers, radiation detectors, 911 system, criminal records, ...
- $>$ 6,000 surveillance cameras, $\frac{2}{3}$ private businesses [33, 75]
- Database of over 16 million plates, every car going into Lower Manhatten [33, 75]
- Can search in seconds for terms like "red baseball cap" [33, 75]
- Detects "suspicious behaviors" like unattended bags and circling cars [33, 75]

Automated License Plate Readers (ALPRs)

[5]

- Scan passing cars' license plates [124, 5]
- Produce alphanumeric representation with timestamp and photograph

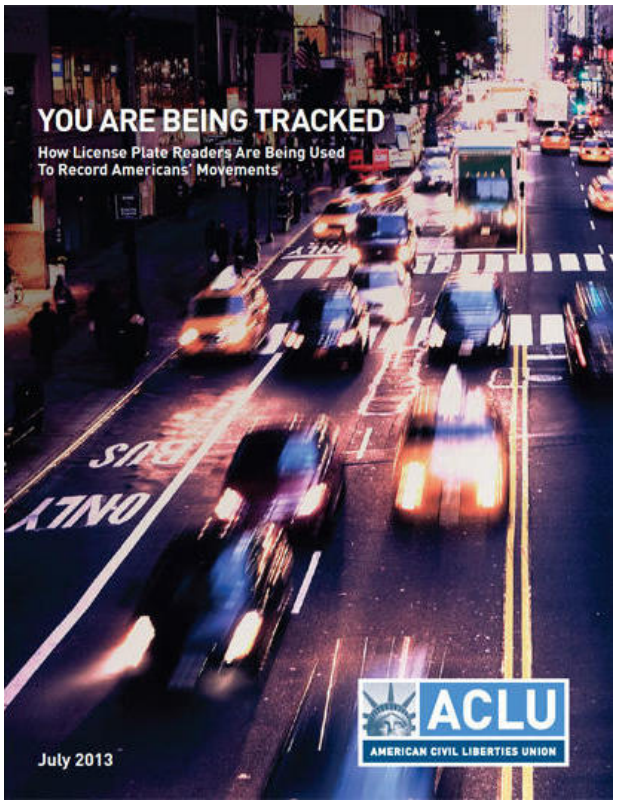
Automated License Plate Readers (ALPRs)



[5]

- Scan passing cars' license plates [124, 5]
- Produce alphanumeric representation with timestamp and photograph

Automated License Plate Readers (ALPRs)



[124]

- Scan passing cars' license plates [124, 5]
- Produce alphanumeric representation with timestamp and photograph

Automatic Toll Readers

- Electronic toll booth using RFIDs or ALPRs [95]
  - In the North-East we have E-ZPass (RFID) [27]
  - Golden Gate Bridge requires FasTrack or plate-based

Automatic Toll Readers

- Electronic toll booth using RFIDs or ALPRs [95]
  - In the North-East we have E-ZPass (RFID) [27]
  - Golden Gate Bridge requires FasTrack or plate-based
  - *But* they provide an option for an anonymous FasTrack account using cash [47]
  - (Granted, you're still captured by an ALPR)

Automatic Toll Readers

- Electronic toll booth using RFIDs or ALPRs [95]
  - In the North-East we have E-ZPass (RFID) [27]
  - Golden Gate Bridge requires FasTrack or plate-based
  - *But* they provide an option for an anonymous FasTrack account using cash [47]
  - (Granted, you're still captured by an ALPR)
- Routinely used by law enforcement [99]
- . . . and divorce cases, in case of FasTrack

Automatic Toll Readers

- Electronic toll booth using RFIDs or ALPRs [95]
  - In the North-East we have E-ZPass (RFID) [27]
  - Golden Gate Bridge requires FasTrack or plate-based
  - *But* they provide an option for an anonymous FasTrack account using cash [47]
  - (Granted, you're still captured by an ALPR)
- Routinely used by law enforcement [99]
- . . . and divorce cases, in case of FasTrack
- They're not very secure—easily cloned either [56, 41]

Akin To GPS Tracking

- *United States v. Jones*: GPS tracking constitutes search under Fourth Amendment [112]
- How is pervasive surveillance different if it achieves essentially the same result?

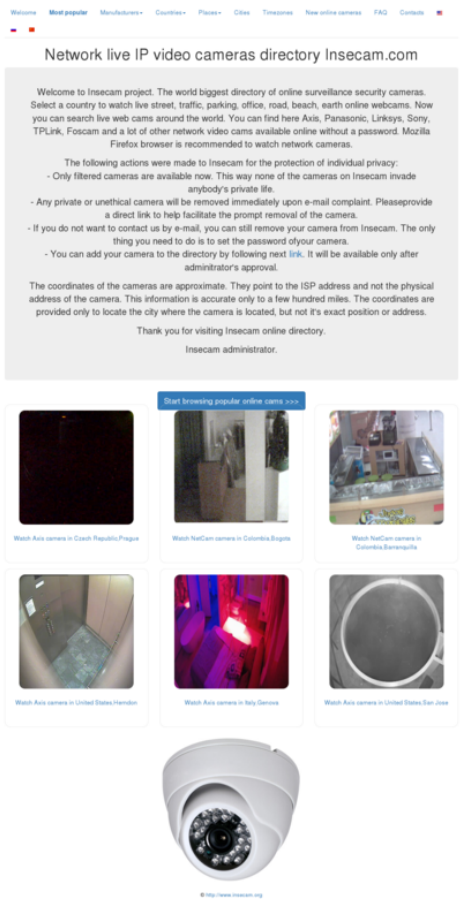
Cameras used to need physical access

Today. . . not always so much

The "S" In IoT Stands For "Security"

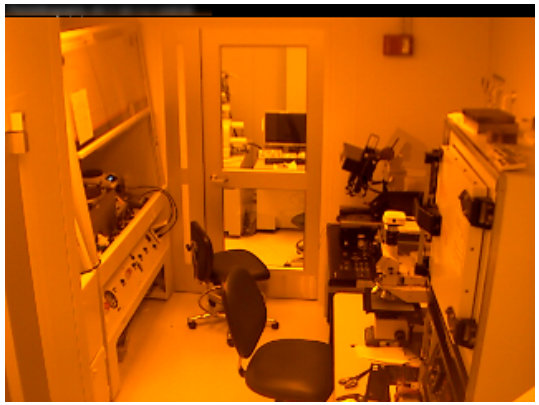
- Shodan—IoT search engine [98]
  - You'll also find other things. Secure your databases. [53]
  - Can search for specific devices
- If you are vulnerable, someone will find you
  - Mirai—620Gbps DDoS Krebs; 1Tbps OVH

Who's Watching?



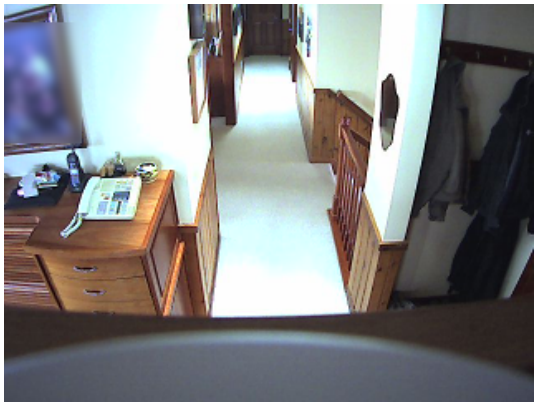
[48]

- Insecam is a directory of Internet-connected surveillance cameras[48]
- Live video feeds (browser connects directly to cameras)




3


3



"Please be aware that if your spoken words include personal or other sensitive information, that information will be among the data captured and transmitted to a third party through your use of Voice Recognition."

—Samsung SmartTV Privacy Policy, 2015

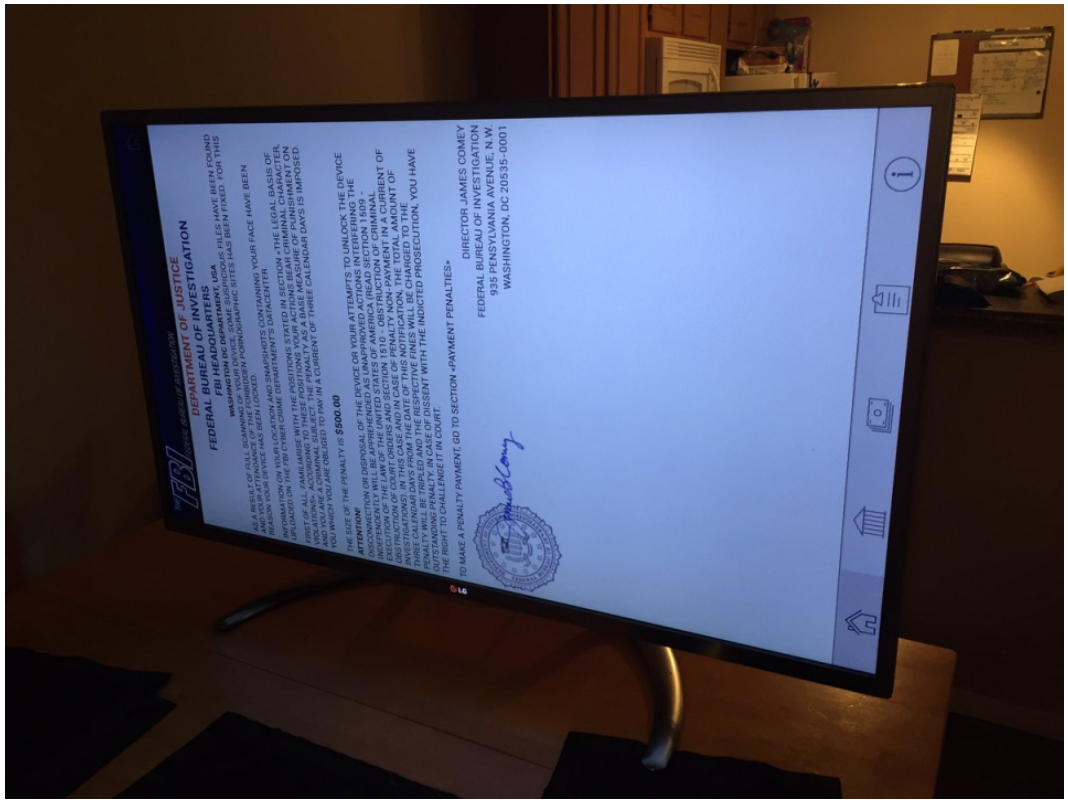
[45]

Weeping Angel

[119, 115]

- Suppress LEDs for “fake off”
- Record audio
- Remote shell and file transfer
- Extract WiFi credentials
- “TODO”: Record video

Smart TV Ransomware (LG)



[18]

Vulnerabilties Equities Process (VEP)

- Whether or not government should disclose vulnerability
- Hoarding is dangerous (Shadow Brokers / Equation Group; Vault 7 / CIA)
- Apple v. FBI

Vulnerabilties Equities Process (VEP)

- Whether or not government should disclose vulnerability
- Hoarding is dangerous (Shadow Brokers / Equation Group; Vault 7 / CIA)
- Apple v. FBI
- Makes us less safe!
  - "Cyberweapon" is an exploit—it cannot be contained

Amazon Echo—Always Listening

[65]

- Voice recognition on Amazon's servers; have recordings [102, 2]
- Warrant issued in murder case for recordings [102, 2]
- Always listening; "wake word" doesn't matter (they control the software; device can be compromised) [73]

Amazon Echo—Always Listening

[65]

- Voice recognition on Amazon's servers; have recordings [102, 2]
- Warrant issued in murder case for recordings [102, 2]
- Always listening; "wake word" doesn't matter (they control the software; device can be compromised) [73]
  - Should do voice recognition on the device
  - Run free software
  - Connect to *your own server* for actions
  - Hardware switch for microphone

Consder the Benign

- Water meter used in murder case as evidence [2]
  - 140 gallons between 1AM and 3AM in Winter?
- Thermostat?
  - Usage patterns could hint at when you're home
- Window/door sensors?

Creepy-Ass Children's Toys?

Germany

German parents told to destroy doll that can spy on children

German watchdog classifies My Friend Cayla doll as 'illegal espionage apparatus' and says shops and owners could face fines

Jayla, aged four, plays with a My Friend Cayla doll in the Hamleys toy shop in London. Photograph: Rob Stothard/Getty Images

This article is **1 month old**

Philip Oltermann

Friday 17 February 2017 16.53 GMT

[76]

Creepy-Ass Children's Toys?

the ONION®???

UK world sport football opinion culture business lifestyle fashion environment tech

home › world › europe US americas asia australia africa middle east cities development

Germany

German parents told to destroy doll that can spy on children

German watchdog classifies My Friend Cayla doll as 'illegal espionage apparatus' and says shops and owners could face fines

This article is **1 month old**

Philip Oltermann

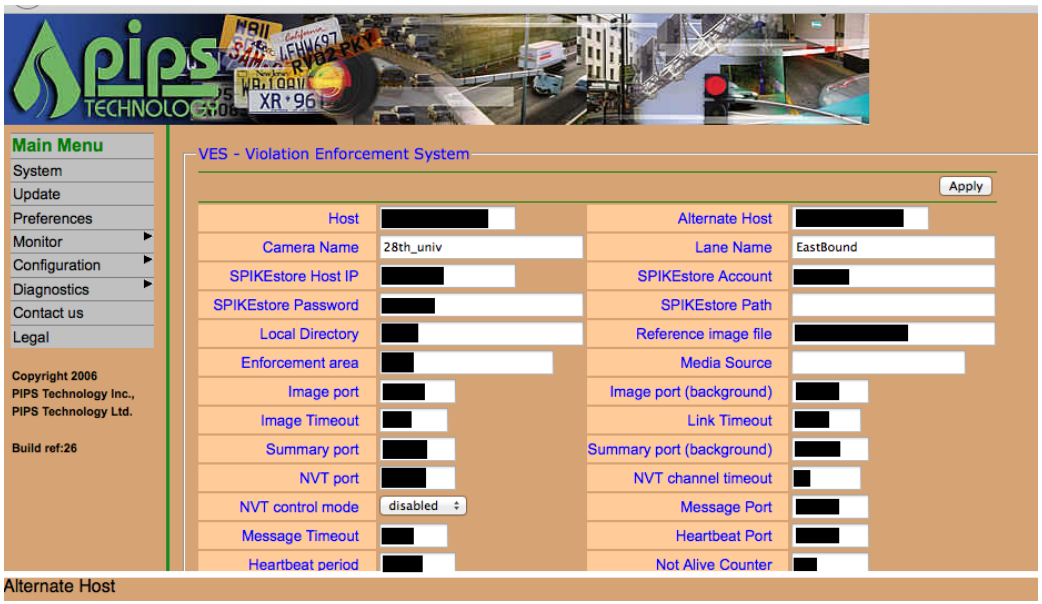
...

Friday 17 February 2017 16.53 GMT

Jayla, aged four, plays with a My Friend Cayla doll in the Hamleys toy shop in London. Photograph: Rob Stothard/Getty Images

[76]

ALPRs Wide Open



[5]

- John Matherly (Shodan author) noticed many web-accessible PIPS control panels
- Other researcher found some accessible via telnet [34]

Biometrics

- Humans no longer need to scour video feeds [96, 17, 28, 75]
- Facial recognition widely used, even for mobile apps [14, 36, 59]

Biometrics

- Humans no longer need to scour video feeds [96, 17, 28, 75]
- Facial recognition widely used, even for mobile apps [14, 36, 59]
  - NYPD has a gallery of over 4M individuals [75]
  - Quality can be low and pixelated; various machine learning algorithms [75, 69, 24]

Biometrics

- Humans no longer need to scour video feeds [96, 17, 28, 75]
- Facial recognition widely used, even for mobile apps [14, 36, 59]
  - NYPD has a gallery of over 4M individuals [75]
  - Quality can be low and pixelated; various machine learning algorithms [75, 69, 24]
- No face? Check your gait. [91, 114]

Biometrics

- Humans no longer need to scour video feeds [96, 17, 28, 75]
- Facial recognition widely used, even for mobile apps [14, 36, 59]
  - NYPD has a gallery of over 4M individuals [75]
  - Quality can be low and pixelated; various machine learning algorithms [75, 69, 24]
- No face? Check your gait. [91, 114]
- No gait? Well. . . whatever, just ask Facebook. [94]

Biometrics

- Humans no longer need to scour video feeds [96, 17, 28, 75]
- Facial recognition widely used, even for mobile apps [14, 36, 59]
  - NYPD has a gallery of over 4M individuals [75]
  - Quality can be low and pixelated; various machine learning algorithms [75, 69, 24]
- No face? Check your gait. [91, 114]
- No gait? Well. . . whatever, just ask Facebook. [94]
- Even fingerprints and iris from high-resolutions photos (defeat Apple's TouchID) [44]

Collateral Damage

- Please don't put pictures of me on Facebook [101]
- Don't put pictures of my children anywhere [22]

Collateral Damage

- Please don't put pictures of me on Facebook [101]
- Don't put pictures of my children anywhere [22]
- That person in the distance is collateral damage [14, 4, 75]

Fleshy You $\Longleftrightarrow$ Virtual You

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

Bureau of Consumer Protection

[date]

BY ELECTRONIC MAIL

[App Developer]

Dear Sir or Madam:

You currently offer a mobile application for download in the Google Play store. We are writing to you today because of code included in the application that may allow third parties to monitor consumers' television viewing for ad targeting or analytics.

[64]

Ultrasound Tracking

$\cdots \iff$ TV $\iff$ Retail Store $\iff$ Mobile $\iff$ Web $\iff \cdots$

- Correlates users across devices; airgap bridge [63, 70]
  - Inaudible to humans
- Could deanonymize (e.g. Tor users) [62, 19]

Ultrasound Tracking

"Silverpush could generate a detailed log of the television content viewed while a user's mobile phone was turned on." [64]

Ultrasound Cross-Device Tracking (uXDT)

- Termed "Ultrasound Cross-Device Tracking" (uXDT) [19, 23]
- Mitigations?

Ultrasound Cross-Device Tracking (uXDT)

- Termed "Ultrasound Cross-Device Tracking" (uXDT) [19, 23]
- Mitigations?
  - SilverDog is a Chromium addon to filter HTML5 audio [63]

Ultrasound Cross-Device Tracking (uXDT)

- Termed "Ultrasound Cross-Device Tracking" (uXDT) [19, 23]
- Mitigations?
  - SilverDog is a Chromium addon to filter HTML5 audio [63]
  - Don't install software that keep secrets (proprietary)
  - Don't run untrusted code on websites (use e.g. NoScript) [40]

Ultrasound Cross-Device Tracking (uXDT)

- Termed "Ultrasound Cross-Device Tracking" (uXDT) [19, 23]
- Mitigations?
  - SilverDog is a Chromium addon to filter HTML5 audio [63]
  - Don't install software that keep secrets (proprietary)
  - Don't run untrusted code on websites (use e.g. NoScript) [40]
  - Turn off your device when not in use
  - Keep device away from other media

Data Analytics

Data Analytics
(Building User Profiles)

Data Analytics
(Building User Profiles)
(Tracking)

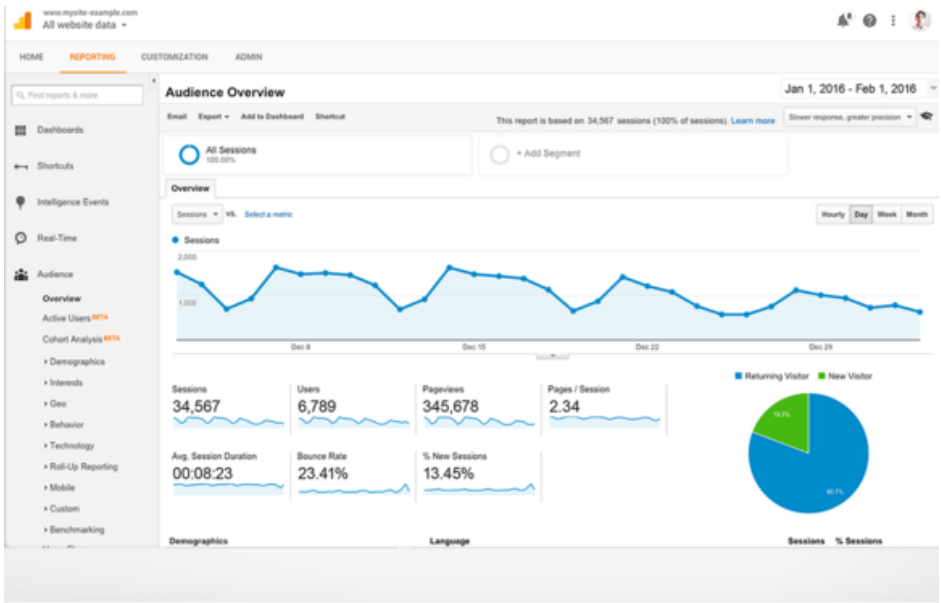
Spyware

Spyware
(With Science)

Trackers

- Website owners want to know what their visitors are doing
  - That in itself isn't an unreasonable concept
- Methods and data define the issue

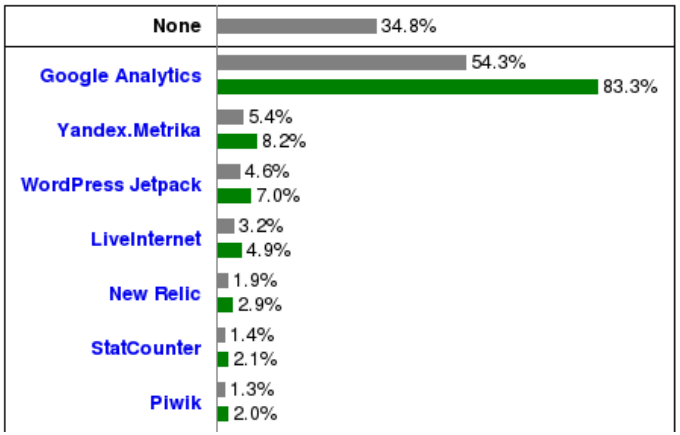
Google Analytics



[60]

- User location, screen resolution, time on page, heatmap, etc [6]
- Unique identifier assigned
- Fine-grained reporting for site owner

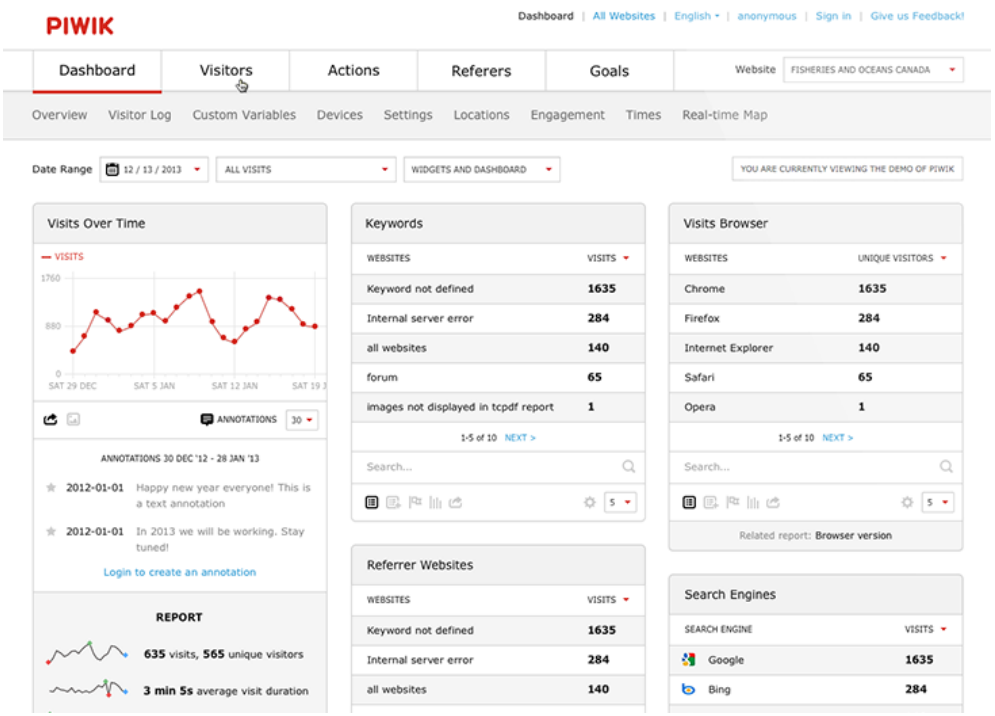
Google Analytics



[113]

- User location, screen resolution, time on page, heatmap, etc [6]
- Unique identifier assigned
- Fine-grained reporting for site owner
- Knows many sites user visited across Web [37]

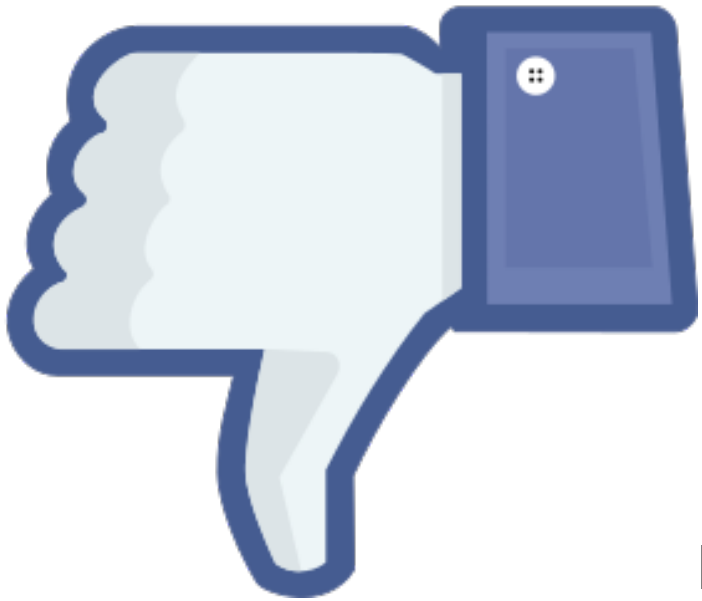
Piwik



[35]

- Data on your own servers [38]
- Visitor privacy settings [118]
- Privacy as a site owner

Like Buttons



[117]

- Infecting the Web with trackers under guise of community [51, 6, 110]
- Tracks regardless of whether you are logged in to Facebook [7, 92, 16]

Fingerprinting

EFF Research, 2010: [49, 46]

"In our analysis of anonymized data from around half a million distinct browsers, 84% had unique configurations. Among browsers that had Flash or Java installed, 94% were unique, and only 1% had fingerprints that were seen more than twice."

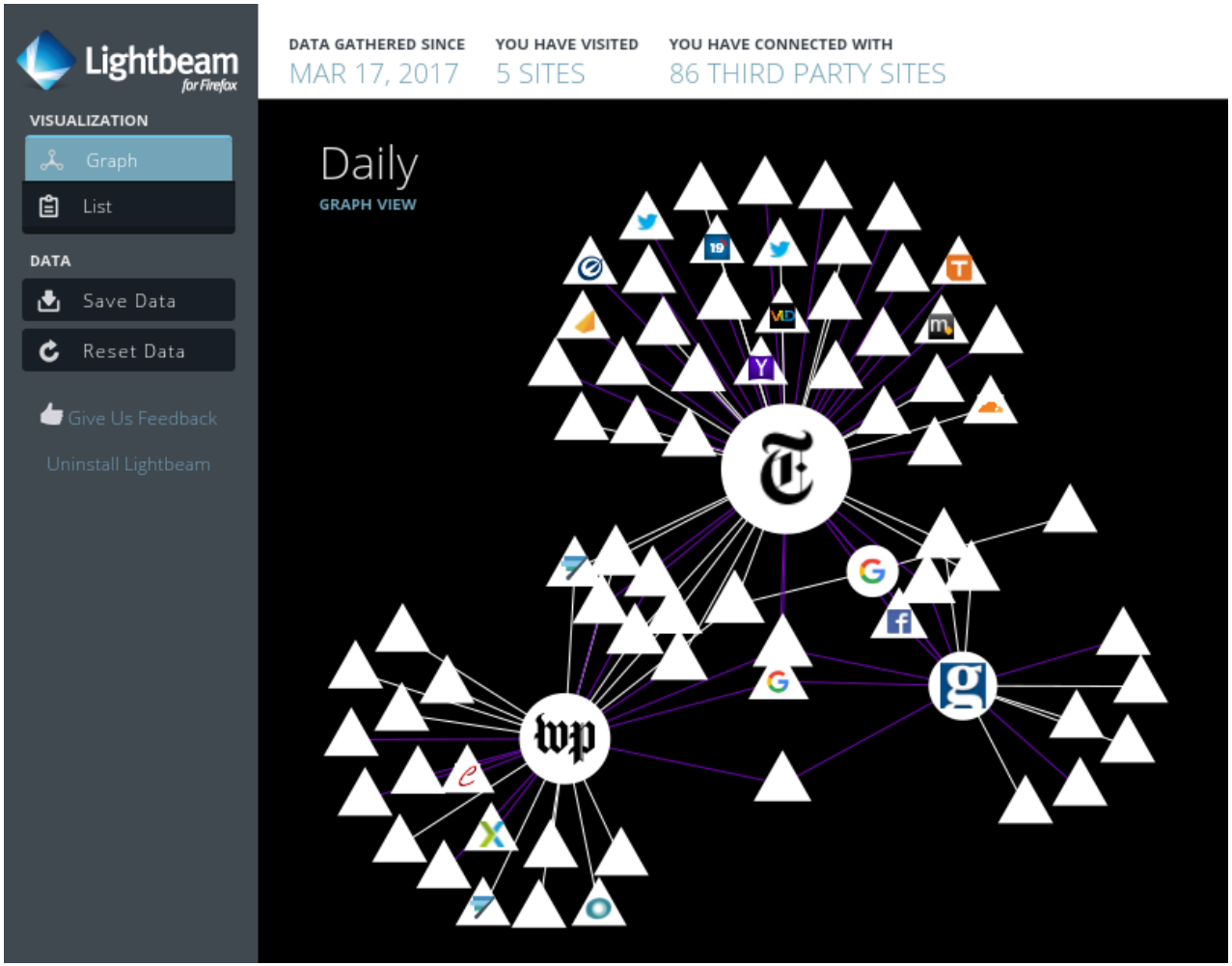
That was seven years ago.
You're really screwed today.*
[10, 46, 31, 50, 81, 1, 71, 9, 42, 12]

Alarmingly Effective

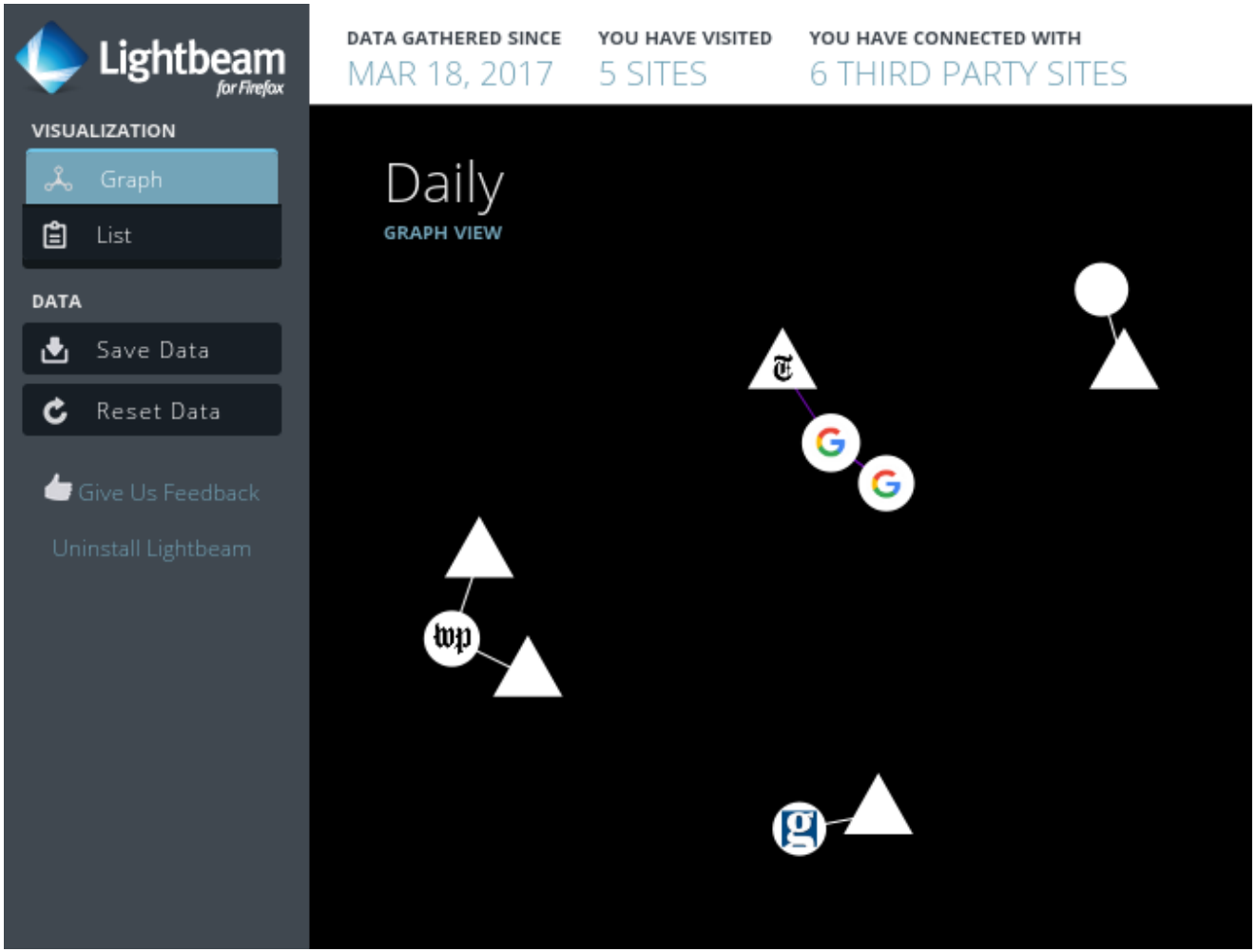
- Panopticlick (EFF) [32]
- User Agent, cookies, screen resolution, fonts, language, session storage, canvas, WebGL, ad blocker, audio, keystrokes, mouse movement, . . . [67]
- Can even track separate browsers on the same hardware [12, 42]

How Does This Happen?

- There is strong incentive to betray
  - Money (advertising)
  - Attention & praise
  - "Business intelligence"


Lightbeam
for Firefox
VISUALIZATION
Graph
List
DATA
Save Data
Reset Data
Give Us Feedback
Uninstall Lightbeam
DATA GATHERED SINCE
MAR 17, 2017
YOU HAVE VISITED
5 SITES
YOU HAVE CONNECTED WITH
86 THIRD PARTY SITES
Daily
GRAPH VIEW

[58]



(After mitigations)

How Do We Mitigate?

Disable the Damn JavaScript!

Disable the Damn JavaScript!

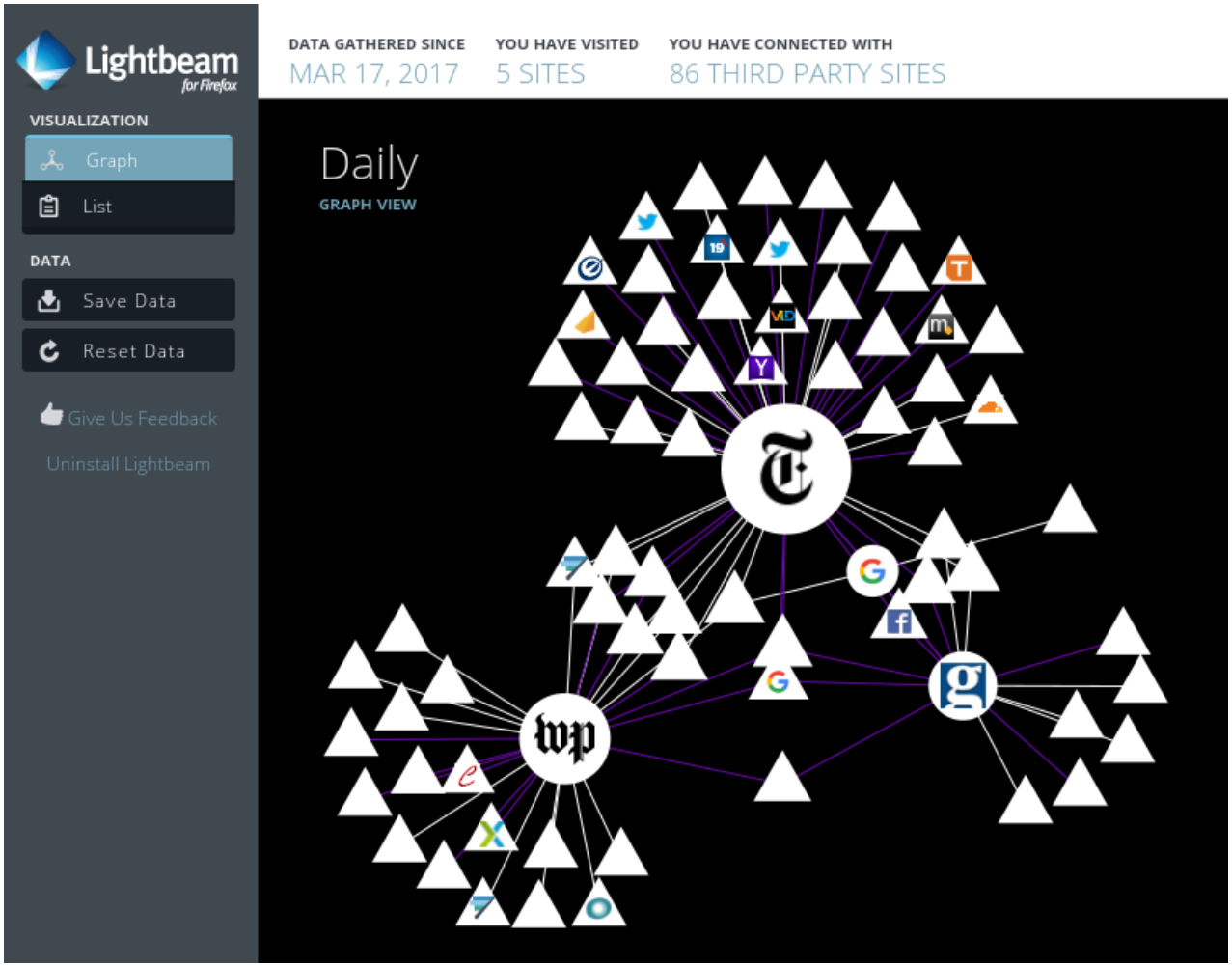
- Preempt most sophisticated and damning fingerprinting methods
  - Stop hardware profiling
  - Stop keystroke/mouse analysis [67]
  - Remember those audio beacons? [19]

Disable the Damn JavaScript!

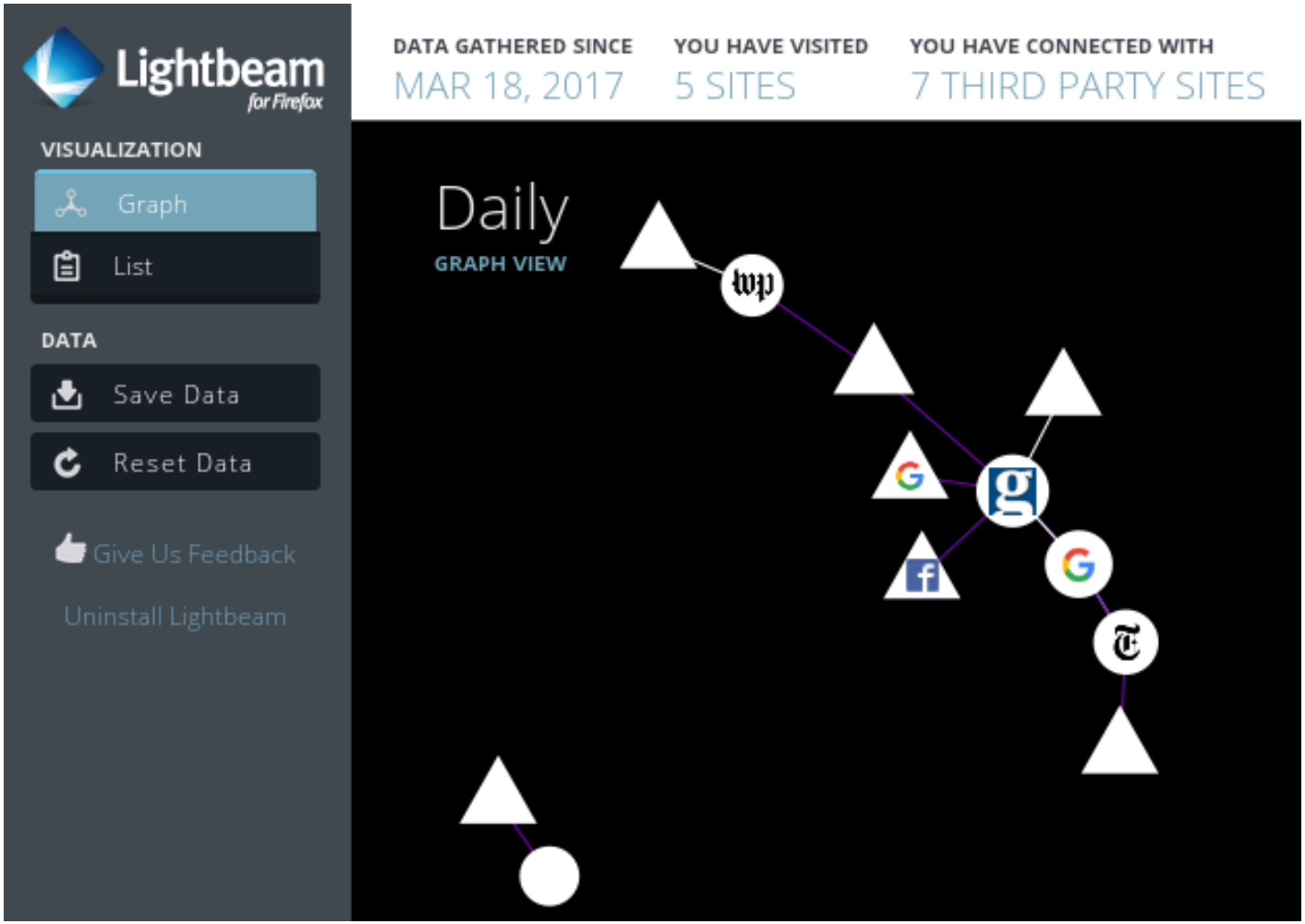
- Running arbitrary untrusted, unsigned, ephemeral code (*also from many third parties*) [40]
  - *Restore Online Freedom!* (My LibrePlanet 2016 talk)
  - LibreJS blocks non-free, but free doesn't mean free of malice

Disable the Damn JavaScript!

- NoScript blocks JavaScript based on URL patterns [72]
  - *Warning:* Allows some sites by default!
  - Also blocks media and fonts; provides XSS and clickjacking prevention

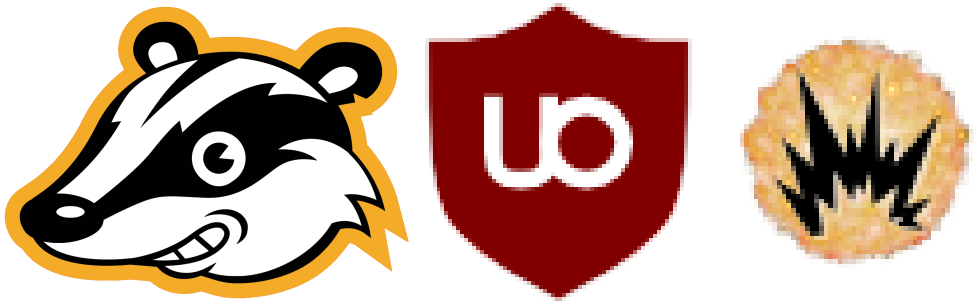


(Before NoScript)



(After NoScript with *no whitelist*)

Ads/Trackers; Security



- *Privacy Badger* blocks trackers [82, 87]
- *uBlock$_0$* "wide-spectrum blocker" [109]
- *Self-Destructing Cookies* clears cookies and LocalStorage [97]


HTTPS://
EVERYWHERE

Pseudonymity

Origin is unknown to server; unique identifier *is available* to server[121]

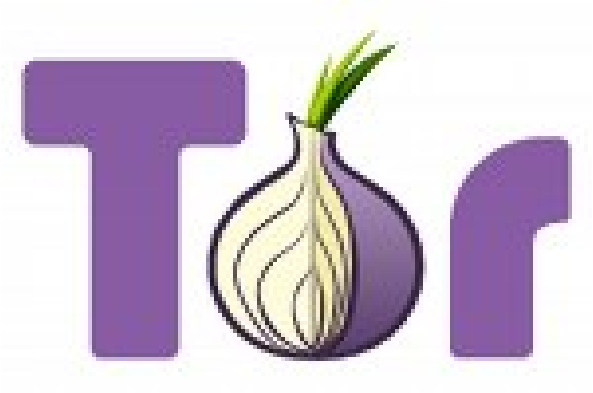
Anonymity

Origin is unknown to server; no unique identifier known by server[121]

IANAAE

(I Am Not An Anonymity Expert)

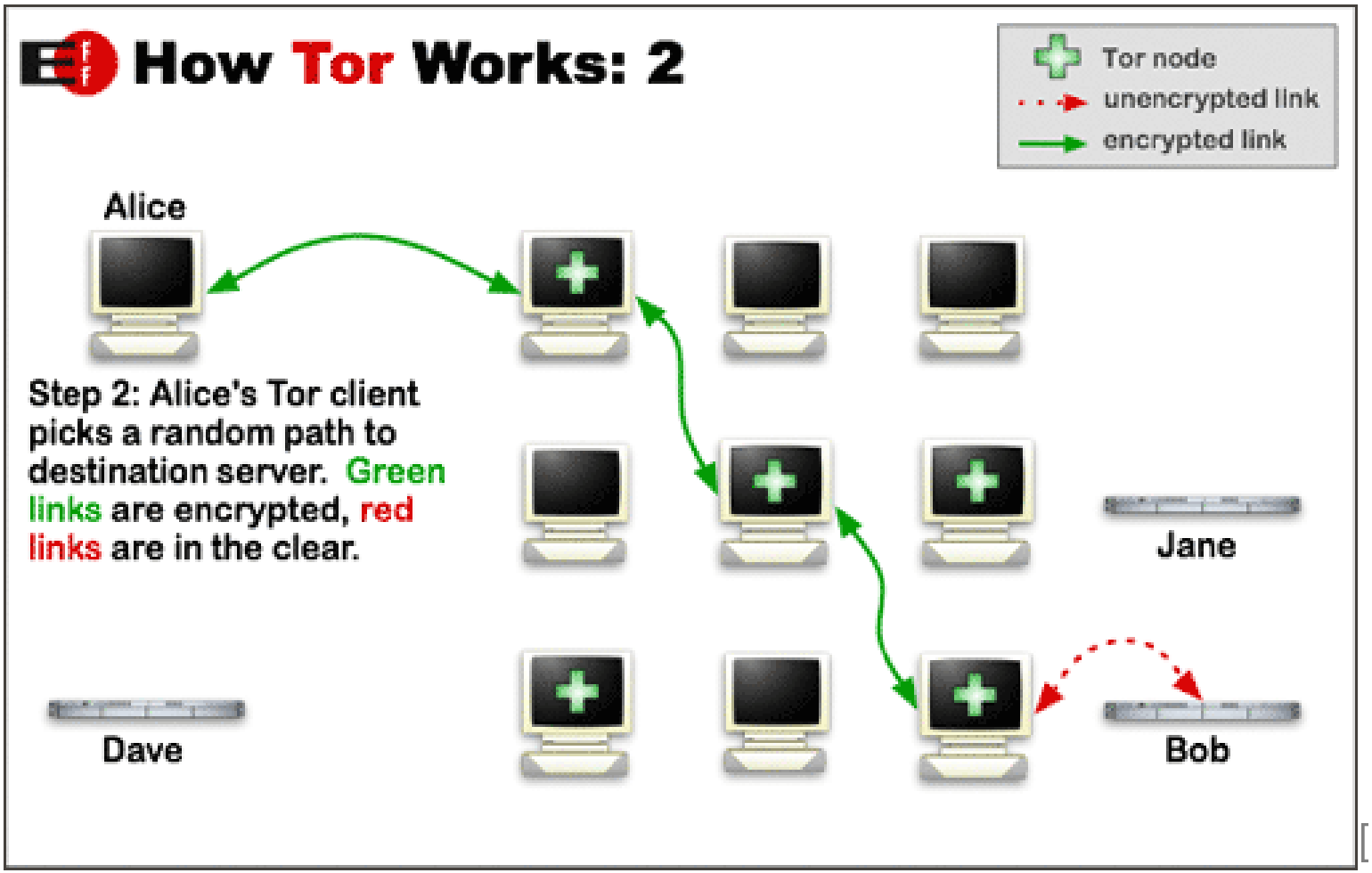
The Tor Network



- The Onion Router (Tor)
- Helps defend against traffic analysis

[85]

The Tor Network



[106]

TorBrowser, Tails, and Whonix

- Also need to change browsing habits [121]

TorBrowser, Tails, and Whonix

- Browser needs to be hardened
  - Remember: browser leaks a lot of data [32, 46]
  - TorBrowser is a hardened Firefox derivative [105, 81]

TorBrowser, Tails, and Whonix

- Operating System needs to be hardened
  - Tails—The Amnesic Incognito Live System

[104]

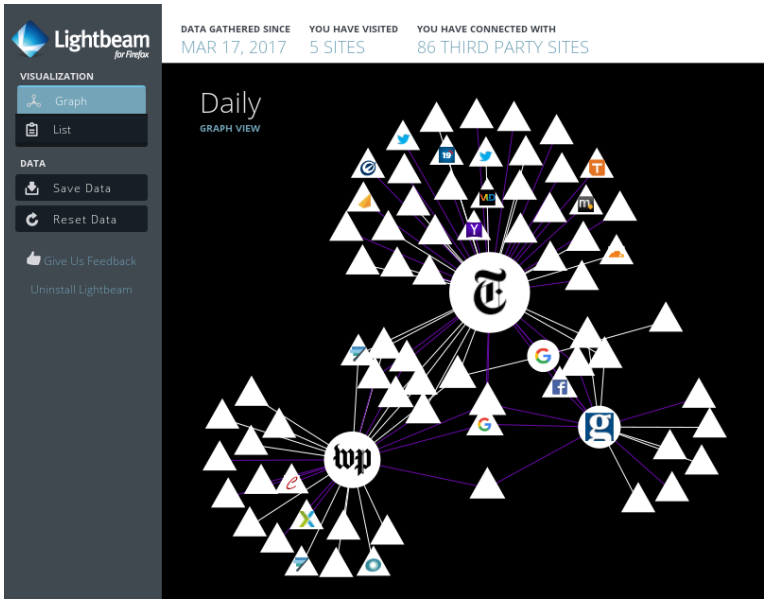
TorBrowser, Tails, and Whonix

- Operating System needs to be hardened
  - Tails—The Amnesic Incognito Live System [104]
  - Whonix—Multi-layer isolation in VMs [122]

"Big Data" (*Your* Big Data)

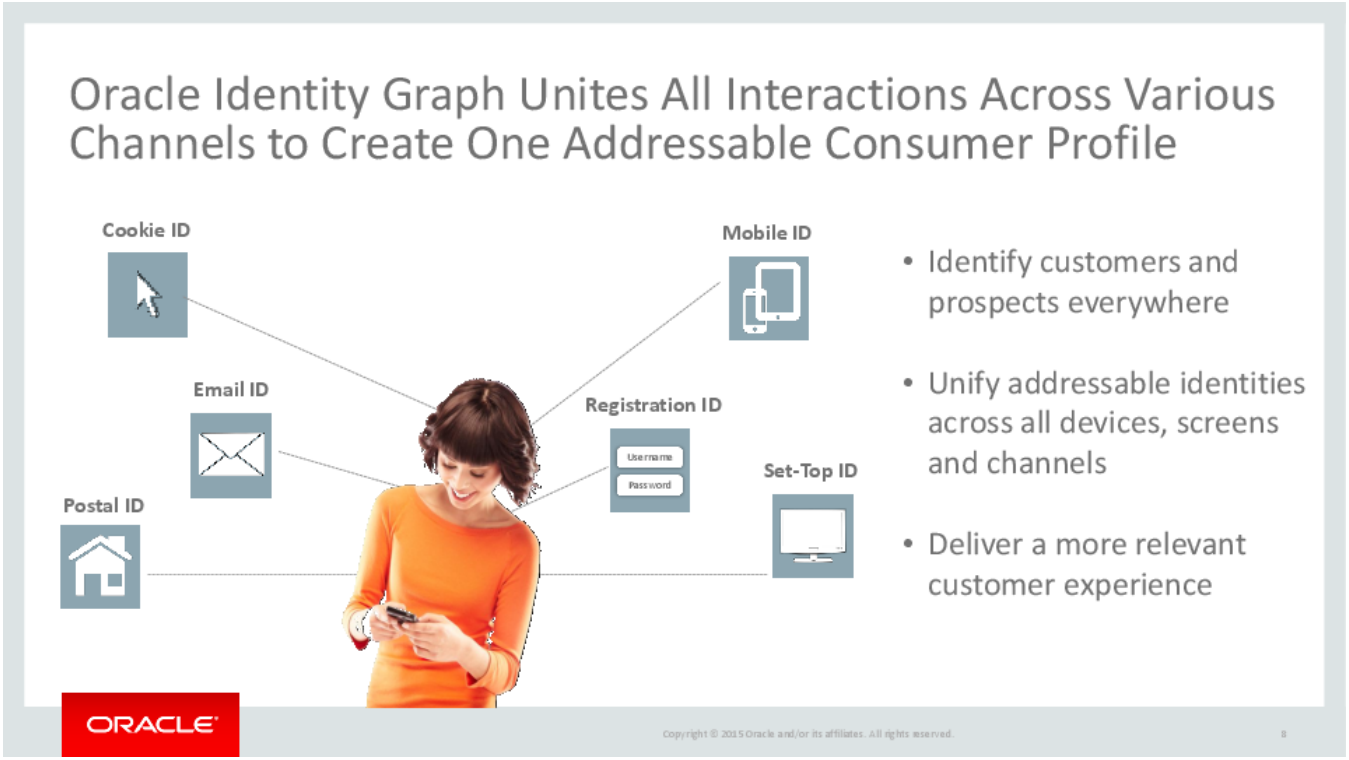
“Business Intelligence”

Data Brokers



- Ghostery lists over 3,000 companies receiving web/app data [21]

Oracle Identity Graph



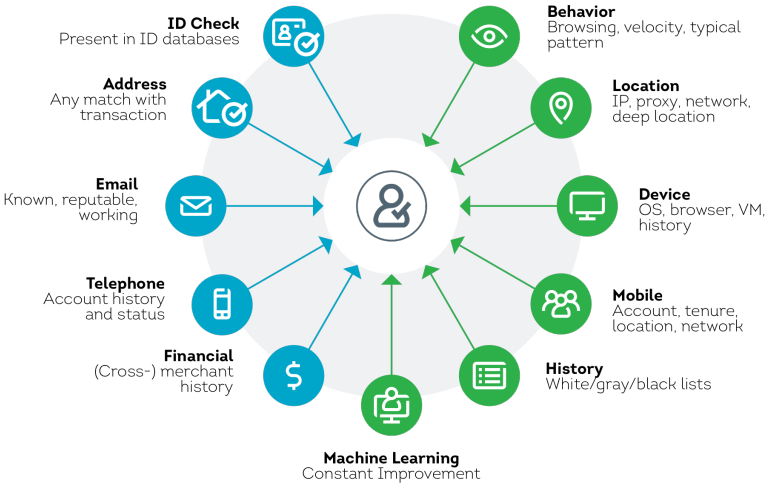
"Aggregates and provides insights on over $2 trillion in consumer spending from 1,500 data partners across 110 million US households" [79]

"More Relevant Customer Experience"

Target Pregnancy Prediction

- Records purchases, credit cards, coupons, surveys, refunds, customer helpline calls, email, website visits, . . . [16]
- Purchase more information from third parties [16]
- Identified 25 products to create a "pregnancy prediction" score and estimate due date [25]
  - Quantities of types of lotions, soaps, cotton balls, supplements, etc

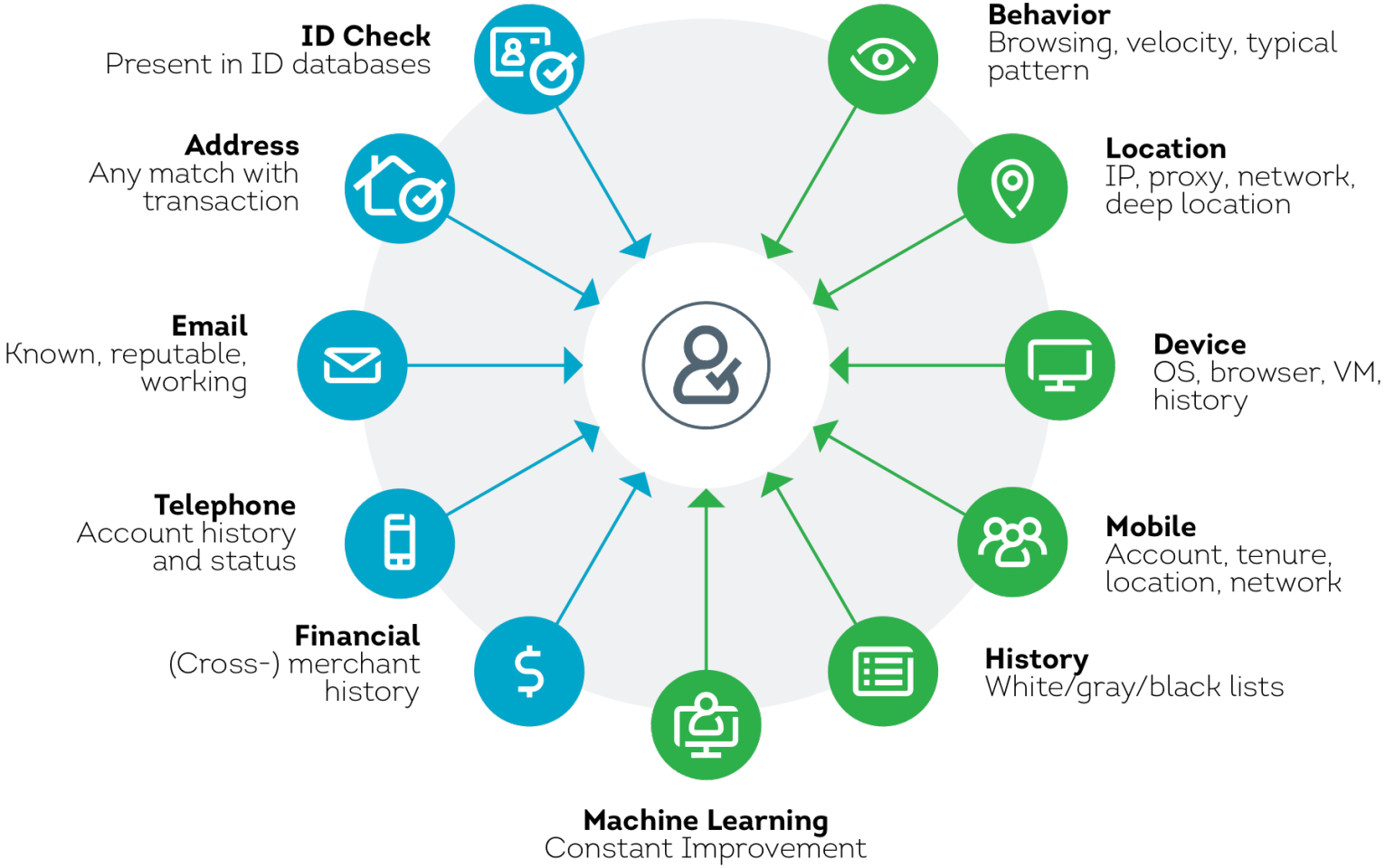
Transparency Needed



[107]

- Let users see their data in this graph!
- Erase nonpublic information that they don't want to be known
- Let them correct what is wrong
  - Also a problem with law enforcement / government
- Let them opt out!

Trustev Fraud Detection



[107]

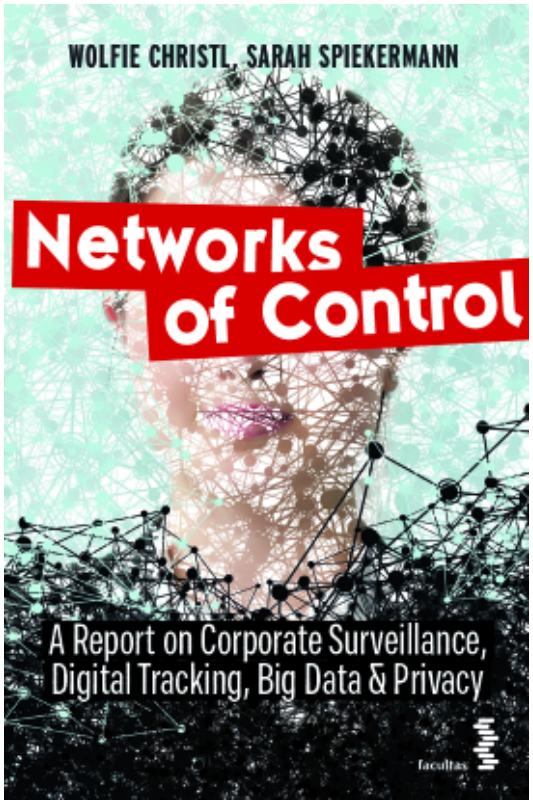
LexisNexis

- Risk management for insurance, finance, retail, travel, government, gaming, and healthcare [16]
- Data on over 500 million customers
- TrueID—34 billion records from over 10,000 sources [57]

"We help insurers assess their risk and streamline the underwriting process in 99% of all U.S. auto insurance claims and more than 90% of all homeowner claims."

Palantir

- Started by Peter Thiel of PayPal
- CIA, DHS, NSA, FBI, the CDC, the Marine Corps, the Air Force, Special Operations Command, West Point, the Joint IED-defeat organization and Allies, the Recovery Accountability and Transparency Board and the National Center for Missing and Exploited Children. [11]



[16, 15]

Shock and Awe

We're feeding into all of this!

Software as a Service Substitute (SaaSS)

- Disturbing trend to replace traditional software with services
- Do not own your own data *or* computations
- Companies balance privacy on their balance sheets
  - Countless data breaches

Decentralize!

- Host what you can (GNU Social, NextCloud, . . .)
- Damnit, Moxie (Signal)—use XMPP, OMEMO

"I Have Nothing To Hide"

Complacency

Complacency in the Status Quo

The status quo cannot hold.

We need to push back

You need to push back

Mike Gerwitz
mtg@gnu.org

References Available Online
https://mikegerwitz.com/talks/sapsf

[1] Gaurav Aggarwal et al. *An Analysis of Private Browsing Modes in Modern Browsers*. Stanford University. URL: https://crypto.stanford.edu/~dabo/pubs/papers/privatebrowsing.pdf (visited on 03/17/2017).

[2] *Amazon refuses to let police access US murder suspect's Echo recordings. Company has declined to provide audio recordings by smart speaker system at house where man died, according to a report*. The Guardian. Dec. 28, 2016. URL: https://www.theguardian.com/technology/2016/dec/28/amazon-refuses-to-let-police-access-suspects-echo-recordings (visited on 03/21/2017).

[3] Thomas Appel. *File:T-mobile cell site*. Wikipedia. Sept. 23, 2015. URL: https://en.wikipedia.org/wiki/File:T-Mobile_cell_site.jpg (visited on 03/19/2017).

[4] Charles Arthur. *Facebook in new privacy row over facial recognition feature. Social network turns on new feature to automatically identify people in photos, raising questions about privacy implications of the service*. The Guardian. June 8, 2011. URL: https://www.theguardian.com/technology/2011/jun/08/facebook-privacy-facial-recognition (visited on 03/12/2017).

[5] *Automated License Plate Readers*. Electronic Frontier Foundation. URL: https://www.eff.org/sls/tech/automated-license-plate-readers (visited on 03/13/2017).

[6] *Behavorial Tracking*. Wikipedia. URL: https://en.wikipedia.org/wiki/Behavioral_targeting (visited on 03/16/2017).

[7] Stephanie Bodoni and John Martens. *Belgium Tells Facebook to Stop Storing Personal Data From Non-Users*. Bloomberg. Nov. 9, 2015. URL: https://www.bloomberg.com/news/articles/2015-11-09/facebook-told-to-stop-storing-personal-data-from-belgian-surfers (visited on 03/16/2017).

[8] Andria Borba. *Nowhere To Hide: Few Public Places Without Surveillance Cameras In San Francisco*. CBS. Sept. 24, 2015. URL: http://sanfrancisco.cbslocal.com/2015/09/24/san-francisco-surveillance-camera-tenderloin/ (visited on 03/12/2017).

[9] *BrowserLeaks.com - Web Browser Security Checklist for Identity Theft Protection*. URL: https://browserleaks.com/ (visited on 03/17/2017).

[10] Bill Budington. *Panopticlick 2.0 Launches, Featuring New Tracker Protection and Fingerprinting Tests*. Electronic Frontier Foundation. Dec. 17, 2015. URL:

https://www.eff.org/deeplinks/2015/12/panopticlick-20-launches-featuring-new-tracker-protection-and-fingerprinting-tests (visited on 03/17/2017).

[11] Matt Burns. *Leaked Palantir Doc Reveals Uses, Specific Functions And Key Clients*. TechCrunch. Jan. 11, 2015. URL: https://techcrunch.com/2015/01/11/leaked-palantir-doc-reveals-uses-specific-functions-and-key-clients/ (visited on 03/19/2017).

[12] Yinshi Cao, Song Li, and Erik Wijmans. "(Cross-)Browser Fingerprinting via OS and Hardware Level Features". In: (2017). DOI: 10.14722/ndss.2017.23152. URL: http://yinzhicao.org/TrackingFree/crossbrowsertracking_NDSS17.pdf (visited on 03/17/2017).

[13] CellularPrivacy. *Android IMSI-Catcher Detector*. URL: https://cellularprivacy.github.io/Android-IMSI-Catcher-Detector/ (visited on 03/11/2017).

[14] Richard Chirgwin. *Facebook conjures up a trap for the unwary: scanning your camera for your friends. Auto-spam your friends with Photo Magic*. The Register. URL: https://web.archive.org/web/20160605165148/http://www.theregister.co.uk/2015/11/10/facebook_scans_camera_for_your_friends/ (visited on 03/12/2017).

[15] Wolfie Christl. *Corporare surveillance, digital tracking, big data & privacy. How thousands of companies are profiling, categorizing, rating and affecting the lives of billions*. Dec. 30, 2016. URL: https://media.ccc.de/v/33c3-8414-corporate_surveillance_digital_tracking_big_data_privacy (visited on 03/18/2017).

[16] Wolfie Christl and Sarah Spiekermann. *Networks of Control*. 2016. URL: http://crackedlabs.org/en/networksofcontrol (visited on 03/18/2017).

[17] *Churchix Facial Recognition Software. Churchix Facial Recognition Software for Event Attendance*. URL: http://churchix.com/ (visited on 03/12/2017).

[18] Catalin Cimpanu. *Android Ransomware Infects LG Smart TV*. Bleeping Computer. URL: https://www.bleepingcomputer.com/news/security/android-ransomware-infects-lg-smart-tv/ (visited on 03/20/2017).

[19] Catalin Cimpanu. *Ultrasound Tracking Could Be Used To Deanonymize Tor Users*. Bleeping Computer. Jan. 3, 2017. URL: https://www.bleepingcomputer.com/news/security/ultrasound-tracking-could-be-used-to-deanonymize-tor-users/ (visited on 03/14/2017).

[20] James R. Clapper. *DNI Statement on Recent Unauthorized Disclosures of Classified Information*. Office of the Director of National Intelligence. June 6, 2013. URL: https://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/868-dni-statement-on-recent-unauthorized-disclosures-of-classified-information (visited on 03/20/2017).

[21] *Company Database*. Ghostery Enterprise. URL: http://www.ghosteryenterprise.com/company-database/ (visited on 03/17/2017).

[22] Josh Constine. *Facebook's New Photo "Scrapbook" Lets Parents Give Kids An Official Presence*. TechCrunch. Mar. 31, 2016. URL: https://techcrunch.com/2015/03/31/step-1-identify-baby-photo-step-2-hide-baby-photos/ (visited on 03/12/2017).

[23] *Cross-Device Tracking*. Federal Trade Commission. Nov. 16, 2015. URL: https://www.ftc.gov/news-events/events-calendar/2015/11/cross-device-tracking (visited on 03/15/2017).

[24] Ryan Dahl, Mohammad Norouzi, and Jonathan Shlens. *Pixel Recursive Super Resolution*. Google Brain. Feb. 2, 2017. arXiv: 1702.00783 [cs.CV].

[25] Charles Duhigg. *How Companies Learn Your Secrets*. The New York Times. Feb. 16, 2016. URL: http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html (visited on 03/19/2017).

[26] Jim Edwards. *Ford Exec: 'We Know Everyone Who Breaks The Law' Thanks To Our GPS In Your Car*. Business Insider. Jan. 8, 2014. URL: http://www.businessinsider.com/ford-exec-gps-2014-1 (visited on 03/21/2017).

[27] *E-ZPass*. Wikipedia. URL: https://en.wikipedia.org/wiki/E-ZPass (visited on 03/13/2017).

[28] *Face Recognition Software for Retail Stores: #1 Biometric Surveillance for Loss Prevention*. URL: https://www.facefirst.com/industry/retail-face-recognition/ (visited on 03/12/2017).

[29] *File:GPS Satellite NASA art-iif.jpg*. NASA. Feb. 9, 2006. URL: https://en.wikipedia.org/wiki/File:GPS_Satellite_NASA_art-iif.jpg (visited on 03/19/2017).

[30] *File:Stingray Harris handle side.jpg*. Harris Corporation. Apr. 2013. URL: https://en.wikipedia.org/wiki/File:Stingray_Harris_handle_side.jpg (visited on 03/19/2017).

[31] *Fingerprinting - MozillaWiki*. Mozilla. URL: https://wiki.mozilla.org/Fingerprinting (visited on 03/17/2017).

[32] Electric Frontier Foundation. *Panopticlick | About*. URL: https://panopticlick.eff.org/about (visited on 03/08/2017).

[33] Chris Francescani. *NYPD expands surveillance net to fight crime as well as terrorism*. Reuters. June 21, 2013. URL: http://www.reuters.com/article/usa-ny-surveillance-idUSL2N0EV0D220130621 (visited on 03/13/2017).

[34] Darius Freamon. *PIPS Technology AUTOPLATE Automatic License Plate Recognition (ALPR) Multiple Vulnerabilities*. URL: https://dariusfreamon.wordpress.com/2014/02/19/pips-technology-autoplate-automatic-license-plate-recognition-alpr-multiple-vulnerabilities/ (visited on 03/14/2017).

[35] *Free Web Analytics Software*. Piwik. URL: https://piwik.org/ (visited on 03/15/2017).

[36] Gennie Gebhart, Starchy Grant, and Erica Portnov. *Facial Recognition, Differential Privacy, and Trade-Offs in Apple's Latest OS Releases*. Electronic Frontier Foundation. Sept. 27, 2016. URL: https://www.eff.org/deeplinks/2016/09/facial-recognition-

differential-privacy-and-trade-offs-apples-latest-os-releases (visited on 03/12/2017).

[37] Matthias Gelbmann. *Google can't track every click of your web surfing. Only most of them.* W3Techs. Feb. 27, 2012. URL: https://w3techs.com/blog/entry/google_cant_track_every_single_click_of_your_web_surfing_only_most_of_them (visited on 03/15/2017).

[38] Mike Gerwitz. *Google Analytics Removed From GitLab.com Instance*. Jan. 24, 2016. URL: https://mikegerwitz.com/2016/01/Google-Analytics-Removed-from-GitLab.com-Instance (visited on 03/16/2017).

[39] Mike Gerwitz. *National Uproar: A Comprehensive Overview of the NSA Leaks and Revelations*. June 2013. URL: https://mikegerwitz.com/2013/06/National-Uproar-A-Comprehensive-Overview-of-the-NSA-Leaks-and-Revelations (visited on 03/09/2017).

[40] Mike Gerwitz. *Restore Online Freedom!* Mar. 20, 2016. URL: https://media.libreplanet.org/u/libreplanet/collection/restore-online-freedom/ (visited on 03/17/2017).

[41] Dan Goodin. *Passport RFIDs cloned wholesale by $250 eBay auction spree$. Video shows you how*. The Register. URL: https://web.archive.org/web/20170127114339/http:

//www.theregister.co.uk/2009/02/02/low_cost_rfid_cloner/ (visited on 03/13/2017).

[42] Dan Goodwin. *Now sites can fingerprint you online even when you use multiple browsers. Online tracking gets more accurate and harder to evade*. Ars Technica. URL: https://arstechnica.co.uk/security/2017/02/now-sites-can-fingerprint-you-online-even-when-you-use-multiple-browsers/ (visited on 03/17/2017).

[43] Glenn Greenwald. *NSA collecting phone records of millions of Verizon customers daily. Exclusive: Top secret court order requiring Verizon to hand over all call data shows scale of domestic surveillance under Obama*. June 6, 2013. URL: https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order (visited on 03/20/2017).

[44] *Hacker extracts Merkel's iris image*. Planet Biometrics. Nov. 30, 2015. URL: http://www.planetbiometrics.com/article-details/i/3644/ (visited on 03/12/2017).

[45] Parker Higgins. *Big Brother Is Listening: Users Need the Ability To Teach Smart TVs New Lessons*. Electronic Frontier Foundation. Feb. 11, 2015. URL: https://www.eff.org/deeplinks/2015/02/big-brother-

listening-users-need-ability-teach-smart-tvs-new-lessons (visited on 03/20/2017).

[46] *How Unique Is Your Web Browser?* Electronic Frontier Foundation. May 17, 2010. URL: https://panopticlick.eff.org/static/browser-uniqueness.pdf (visited on 03/17/2017).

[47] *I Want To Remain Anonymous*. Golden Gate Bridge, Highway and Transportation District. URL: http://goldengate.org/tolls/iwanttoremainanonymous.php (visited on 03/13/2017).

[48] *Insecam - World biggest online cameras directory*. URL: http://insecam.org (visited on 03/19/2017).

[49] *Is Every Browser Unique? Results Fom The Panopticlick Experiment*. Electronic Frontier Foundation. May 17, 2010. URL: https://www.eff.org/deeplinks/2010/05/every-browser-unique-results-fom-panopticlick (visited on 03/17/2017).

[50] Artur Janc and Michal Zalewski. *Technical analysis of client identification mechanisms*. Google. URL: https://sites.google.com/a/chromium.org/dev/Home/chromium-security/client-identification-mechanisms (visited on 03/17/2017).

[51] Michal Kosinski, David Stillwell, and Thore Graepel. "Private traits and attributes are predictable from digital records of human behavior". In: *PNAS* 110 (Feb. 12, 2013), pp. 5802–5805. DOI: 10.1073/pnas.1218772110. URL: http://www.pnas.org/content/110/15/5802.full.pdf (visited on 03/16/2017).

[52] Manikanta Kotaru et al. "SpotFi: Decimeter Level Localization Using WiFi". In: *ACM SIGCOMM Computer Communication Review - SIGCOMM'15* 45 (2015), pp. 269–282. DOI: 10.1145/2785956.2787487.

[53] Brian Krebs. *Extortionists Wipe Thousands of Databases, Victims Who Pay Up Get Stiffed*. URL: https://krebsonsecurity.com/2017/01/extortionists-wipe-thousands-of-databases-victims-who-pay-up-get-stiffed/ (visited on 03/12/2017).

[54] Kryptowire. *KRYPTOWIRE DISCOVERS MOBILE PHONE FIRMWARE THAT TRANSMITTED PERSONALLY IDENTIFIABLE INFORMATION (PII) WITHOUT USER CONSENT OR DISCLOSURE*. URL: http://www.kryptowire.com/adups_security_analysis.html (visited on 03/11/2017).

[55] Swarun Kumar et al. "LTE radio analytics made easy and accessible". In: *S3 '14 Proceedings of the 6th annual workshop on Wireless of the students, by*

the students, for the students (2014), pp. 29–30. DOI: 10.1145/2645884.2645891.

[56] Nate Lawson. *Highway To Hell: Hacking Toll Systems*. Aug. 6, 2008. URL: http://www.root.org/talks/BH2008_HackingTollSystems.pdf (visited on 03/13/2017).

[57] *LexisNexis TrueID*. LexisNexis. URL: http://www.lexisnexis.com/risk/downloads/literature/trueid.pdf (visited on 03/18/2017).

[58] *Lightbeam for Firefox. Shine a Light on Who's Watching You*. Mozilla. URL: https://www.mozilla.org/en-US/lightbeam/ (visited on 03/17/2017).

[59] Jennifer Lynch. *New Report: FBI Can Access Hundreds of Millions of Face Recognition Photos*. Electronic Frontier Foundation. June 15, 2016. URL: https://www.eff.org/deeplinks/2016/06/fbi-can-search-400-million-face-recognition-photos (visited on 03/12/2017).

[60] *Marketing Data Analysis & Reporting Features*. Google. URL: https://www.google.com/analytics/analytics/features/ (visited on 03/15/2017).

[61] Jeremy Martin et al. *A Study of MAC Address Randomization in Mobile Devices and When it Fails*. Mar. 2017. arXiv: 1703.02874 [cs.CR].

[62] Vasillios Mavroudis and Federico Maggi. *Talking Behind Your Back. On the Privacy & Security of the Ultrasound Tracking Ecosystem*. Dec. 29, 2016. URL: https://media.ccc.de/v/33c3-8336-talking_behind_your_back (visited on 03/14/2017).

[63] V. Mavroudis et al. *The Ultrasound Tracking Ecosystem*. URL: http://ubeacsec.org/downloads/report.pdf (visited on 03/14/2017).

[64] Maneesha Mithal. *Sample Silverpush Letter*. United States Federal Trade Commission, Bureau of Consumer Protection, Divison of Privacy and Identity Protection. URL: https://www.ftc.gov/system/files/attachments/press-releases/ftc-issues-warning-letters-app-developers-using-silverpush-code/160317samplesilverpushltr.pdf (visited on 03/14/2017).

[65] Frank Morrison. *File:Amazon Echo.jpg*. Wikipedia. Oct. 17, 2014. URL: https://en.wikipedia.org/wiki/File:Amazon_Echo.jpg (visited on 03/21/2017).

[66] MozillaWiki. *CloudServices/Location - MozillaWiki*. URL: https://wiki.mozilla.org/CloudServices/Location (visited on 03/11/2017).

[67] Smita S. Mudholkar, Pradnya M. Shende, and Milind V. Sarode. "Biometrics Authentication Technique for Intrustion Detection Systems Using Fingerprint Recognition". In: *International Journal of Computer Science, Engineering and Information Technology* 2.4 (Feb. 2012). DOI: 10.5121/ijcseit.2012.2106. URL: http://airccse.org/journal/ijcseit/papers/2112ijcseit06.pdf (visited on 03/19/2017).

[68] Ashitha Nagesh. *A Tory MP might have quoted Goebbels in defence of the government's surveillance bill*. Metro.co.uk. URL: http://metro.co.uk/2015/11/05/a-tory-mp-might-have-quoted-goebbels-in-defence-of-the-governments-surveillance-bill-5481457/ (visited on 03/13/2017).

[69] Lily Hay Newman. *AI Can Recognize Your Face Even If You're Pixelated*. Wired. Sept. 12, 2016. URL: https://www.wired.com/2016/09/machine-learning-can-identify-pixelated-faces-researchers-show/ (visited on 03/13/2017).

[70] Lily Hay Newman. *How to Block the Ultrasonic Signals You Didn't Know Were Tracking You*. Wired. Nov. 3, 2016. URL: https://www.wired.com/2016/11/block-ultrasonic-signals-didnt-know-tracking/ (visited on 03/14/2017).

[71] Jose Carlos Norte. *Advanced Tor Browser Fingerprinting*. Mar. 6, 2016. URL: http://jcarlosnorte.com/security/2016/03/06/advanced-tor-browser-fingerprinting.html (visited on 03/17/2017).

[72] *NoScript - JavaScript/Java/Flash blocker for a safer Firefox experience!* URL: https://noscript.net/ (visited on 03/17/2017).

[73] Matt Novak. *The FBI Can Neither Confirm Nor Deny Wiretapping Your Amazon Echo*. Gizmodo. May 11, 2016. URL: https://paleofuture.gizmodo.com/the-fbi-can-neither-confirm-nor-deny-wiretapping-your-a-1776092971 (visited on 03/21/2017).

[74] *NSA Spying*. Electronic Frontier Foundation. URL: https://www.eff.org/nsa-spying (visited on 03/20/2017).

[75] Michael O'Brien and Julia Cort. *Manhunt—Boston Bombers. Which technologies worked—and which didn't—in the race to track down the men behind the marathon attack?* WGBH Educational Foundation. May 29, 2013. URL: http://www.pbs.org/wgbh/nova/tech/manhunt-boston-bombers.html (visited on 03/13/2017).

[76] Philip Oltermann. *German parents told to destroy doll that can spy on children. German watchdog classifies My Friend Cayla doll as 'illegal espionage apparatus' and says shop owners could face fines*. The Guardian.

Feb. 17, 2017. URL: https://www.theguardian.com/world/2017/feb/17/german-parents-told-to-destroy-my-friend-cayla-doll-spy-on-children (visited on 03/22/2017).

[77] *OpenMobileNetwork*. URL: http://www.openmobilenetwork.org/ (visited on 03/11/2017).

[78] Kurt Opsahl. *Why Metadata Matters*. Electronic Frontier Foundation. June 7, 2013. URL: https://www.eff.org/deeplinks/2013/06/why-metadata-matters (visited on 03/20/2017).

[79] *Oracle Buys Datalogix. Creates the World's Most Valuable Data Cloud to Maximize the Power of Digital Marketing*. Oracle. URL: http://www.oracle.com/us/corporate/acquisitions/datalogix/general-presentation-2395307.pdf (visited on 03/18/2017).

[80] *OsmAnd - Offline Mobile Maps and Navigation*. URL: http://osmand.net/ (visited on 03/11/2017).

[81] Mike Perry et al. *The Design and Implementation of the Tor Browser*. Tor Project. Mar. 10, 2017. URL: https://www.torproject.org/projects/torbrowser/design/ (visited on 03/17/2017).

[82] *Privacy Badger*. Electronic Frontier Foundation. URL: https://www.eff.org/privacybadger (visited on 03/17/2017).

[83] *Privacy Statement*. OnStar. Jan. 1, 2017. URL: https://www2.onstar.com/tunnel-web/webdav/portal/document_library/tcps/us/ps/web/20140601/en/html/privacy_statement.html (visited on 03/21/2017).

[84] GNU Project. *Malware in Mobile Devices*. URL: https://www.gnu.org/philosophy/malware-mobiles.html (visited on 03/11/2017).

[85] Tor Project. *Tor Project: Anonymity Online*. URL: http://torproject.org/ (visited on 03/09/2017).

[86] *Public Security Privacy Guidelines*. URL: http://www.nyc.gov/html/nypd/downloads/pdf/crime_prevention/public_security_privacy_guidelines.pdf (visited on 03/13/2017).

[87] Cooper Quintin. *Ending Online Tracking! Privacy Badger and Beyond!* Electronic Frontier Foundation. URL: https://media.libreplanet.org/u/libreplanet/m/ending-online-tracking-privacy-badger-and-beyond/ (visited on 03/17/2017).

[88] Replicant. *Freedom and privacy/security issues*. URL: http://www.replicant.us/freedom-privacy-security-issues.php (visited on 03/11/2017).

[89] Replicant. *Replicant*. URL: http://www.replicant.us (visited on 03/11/2017).

[90] Replicant. *Samsung Galaxy back-door*. URL: http://redmine.replicant.us/projects/replicant/wiki/SamsungGalaxyBackdoor (visited on 03/11/2017).

[91] Grégory Rogez, Jonathan Rihan, and Jose J. Guerrero. "Monocular 3D Gait Tracking in Surveillance Scenes". In: *IEEE Transactions on Cybernetics* (). URL: http://vision.ics.uci.edu/papers/RogezRGO_Cybernetics_2013/RogezRGO_Cybernetics_2013.pdf.

[92] Arnold Roosendaal. "Facebook Tracks and Traces Everyone: Like This!" In: *Tilburg Law School Legal Studies Research Paper Series* (2010). DOI: 10.2139/ssrn.1717563. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1717563 (visited on 03/17/2017).

[93] Jeffrey Rosen. *The Naked Crowd: Reclaiming Security and Freedom In An Anxious Age*. Random House, 2004. ISBN: 978-0375508004.

[94] Aviva Rutkin. *Facebook can recognize you in photos even if you're not looking*. New Scientist. URL: https://www.newscientist.com/article/dn27761-facebook-can-recognise-you-in-photos-even-if-youre-not-looking/ (visited on 03/12/2017).

[95] Seth Schoen. *The Golden Gate Bridge Is Watching You*. Electronic Frontier Foundation. Mar. 28, 2013. URL: https://www.eff.org/deeplinks/2013/03/golden-gate-bridge-watching-you (visited on 03/13/2017).

[96] Adam Schwartz. *The Danger of Corporate Facial Recognition Tech. The Illinois Biometric Privacy Statute Survived a Recent Attack. But the Struggle Continues*. Electronic Frontier Foundation. June 7, 2016. URL: https://www.eff.org/deeplinks/2016/06/danger-corporate-facial-recognition-techgg (visited on 03/12/2017).

[97] *Self-Destructing Cookies*. URL: https://addons.mozilla.org/en-US/android/addon/self-destructing-cookies/ (visited on 03/17/2017).

[98] *Shodan. The search engine for the Internet of Things*. URL: https://shodan.io (visited on 03/12/2017).

[99] John Simerman. *Lawyers dig into FasTrak data*. Bay Area News Group. June 5, 2007. URL: http://www.eastbaytimes.com/2007/06/05/lawyers-dig-into-fastrak-data/ (visited on 03/13/2017).

[100] Daniel J. Solove. ""I've got nothing to hide" and Other Misunderstandings of Privacy". In: *San Diego Law Review* 44 (2007), pp. 745–772. URL: https://ssrn.com/abstract=998565 (visited on 03/13/2017).

[101] Richard Stallman. *Reasons not to use (i.e., be used by) Facebook*. URL: https://stallman.org/facebook.html (visited on 03/12/2017).

[102] Billy Steele. *Policy seek Amazon Echo data in murder case*. Engadget. Dec. 27, 2016. URL: https://www.engadget.com/2016/12/27/amazon-echo-audio-data-murder-case/ (visited on 03/21/2017).

[103] *Summary of Voluminous Evidence, Jewel v. NSA, Case No. 08-CV-4373-JSW*. Dec. 14, 2012. URL: https://www.eff.org/files/filenode/jewel_conformed_summary_of_evidence.pdf (visited on 03/20/2017).

[104] *Tails - Privacy for anyone anywhere*. Tor Project. URL: https://tails.boum.org/ (visited on 03/18/2017).

[105] *Tor Browser*. Tor Project. URL: https://www.torproject.org/projects/torbrowser.html.en (visited on 03/17/2017).

[106] *Tor Project: Overview*. Tor Project. URL: https://www.torproject.org/about/overview.html.en (visited on 03/17/2017).

[107] *TransUnion | Trustev – Technology*. TransUnion. URL: http://www.trustev.com/technology (visited on 03/19/2017).

[108] *Trilateration*. Wikipedia. URL: https://en.wikipedia.org/wiki/Trilateration (visited on 03/11/2017).

[109] *uBlock Origin. An efficient blocker for Chromium and Firefox. Fast and lean.* URL: https://github.com/gorhill/uBlock (visited on 03/17/2017).

[110] *ULD to website owners: "Deactivate Facebook web analytics"*. Unabh angiges Landeszentrum fur Datenschutz Schleswig-Holstein. Aug. 19, 2011. URL: https://www.datenschutzzentrum.de/presse/20110819-facebook-en.htm (visited on 03/17/2017).

[111] Neal Ungerleider. *NYPD, Microsoft Launch All-Seeing "Domain Awareness System" With Real-Time CCTV, License Plate Monitoring. The New York Police Department has a new terrorism detection system that will also generate profit for the city*. Fast Company. Aug. 8, 2012. URL: https://www.fastcompany.com/3000272/nypd-microsoft-launch-all-seeing-domain-awareness-system-real-time-cctv-license-plate-monito (visited on 03/13/2017).

[112] *United States v. Jones*. Wikipedia. URL: https://en.wikipedia.org/wiki/United_States_v._Antoine_Jones (visited on 03/13/2017).

[113] *Usage Stastics and Market Share of Traffic Analysis Tools for Websites*. W3Techs. URL: https://w3techs.com/technologies/overview/traffic_analysis/all (visited on 03/15/2017).

[114] Sonali Vaidya and Kamal Shah. "Real Time Video Surveillance System". In: *International Journal of Computer Applications* 86 (2014), pp. 22–27. URL: http://research.ijcaonline.org/volume86/number14/pxc3893419.pdf.

[115] *Vault 7: CIA Hacking Tools Revealed*. Wikileaks. URL: https://wikileaks.org/ciav7p1/index.html (visited on 03/21/2017).

[116] Roger Vinson. *Foreign Intelligence Surveillance Court Ruling- Verizon*. United States Foreign Intelligence Surveillance Court. Apr. 25, 2013. URL: https://archive.org/details/FBI-Verizon-FISA-2013 (visited on 03/20/2017).

[117] Enoc Vt. *File:Botón Me gusta.svg*. Oct. 9, 2011. URL: https://en.wikipedia.org/wiki/File:Bot%C3%83%C2%B3n_Me_gusta.svg (visited on 03/16/2017).

[118] *Web Analytics Privacy in Piwik*. Piwik. URL: https://piwik.org/privacy/ (visited on 03/15/2017).

[119] *Weeping Angel (Extending) Engineering Notes, SECRET // REL USA,UK*. Central Intelligence Agency. URL: https://wikileaks.org/ciav7p1/cms/page_12353643.html (visited on 03/20/2017).

[120] *What They Know - Mobile - WSJ*. The Wall Street Journal. URL: http://blogs.wsj.com/wtk-mobile/ (visited on 03/19/2017).

[121] Whonix. *DoNot*. URL: https://www.whonix.org/wiki/DoNot (visited on 03/05/2017).

[122] *Whonix*. Whonix. URL: https://www.whonix.org/ (visited on 03/18/2017).

[123] *Wi-Fi positioning system*. Wikipedia. URL: https://en.wikipedia.org/wiki/Wi-Fi_positioning_system (visited on 03/11/2017).

[124] *You Are Being Tracked. How License Plate Readers Are Being Used To Record Americans' Movements*. URL: https://www.aclu.org/sites/default/files/field_document/071613-aclu-alprreport-opt-v05.pdf (visited on 03/13/2017).

[125] Jinyan Zang et al. *Who Knows What About Me? A Survey of Behind the Scenes Personal Data Sharing to Third Parties by Mobile Apps*. URL: http://jots.pub/a/2015103001/index.php (visited on 03/11/2017).