Digital Marketing

urrent Techniques, Choices, nd Privacy Controls

he Future of Marketing in the ra of Trump and Brexit

.26.16

FUTURE OF PRIVACY FORUM

uture of Privacy Forum

he Future of Privacy Forum is a non-profit organization
at serves as a catalyst for privacy leadership and
cholarship, advancing principled data practices in support
emerging technologies.

rojects: Big Data, De-Identification, Ethics, Wearables,
onnected Cars, Ed Tech, Location and Ad Tech, Smart
ties, Drones, Facial Recognition

POs, Academics and Civil Society

FUTURE OF PRIVACY FORUM

ules Polonetsky, *CEO*

ormer Chief Privacy Officer AOL and
oubleClick

ormer Consumer Affairs Commissioner,
ity of NY

ormer State Legislator

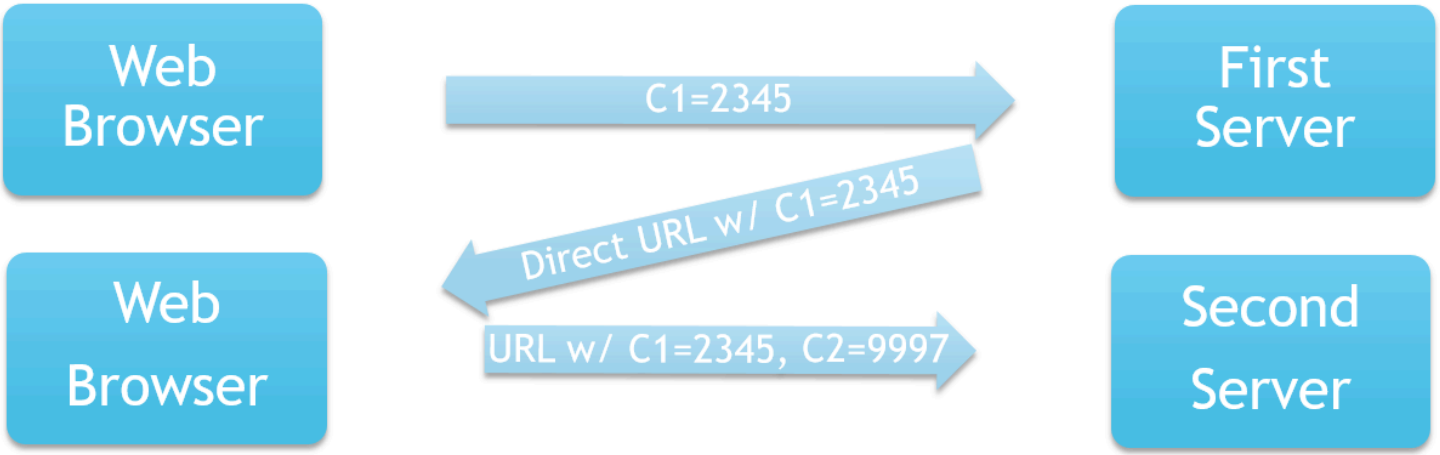
Jules Polonetsky, CEO
julespol@fpf.org

- www.fpf.org
- facebook.com/futureofprivacy
- @futureofprivacy

FUTURE OF PRIVACY FORUM

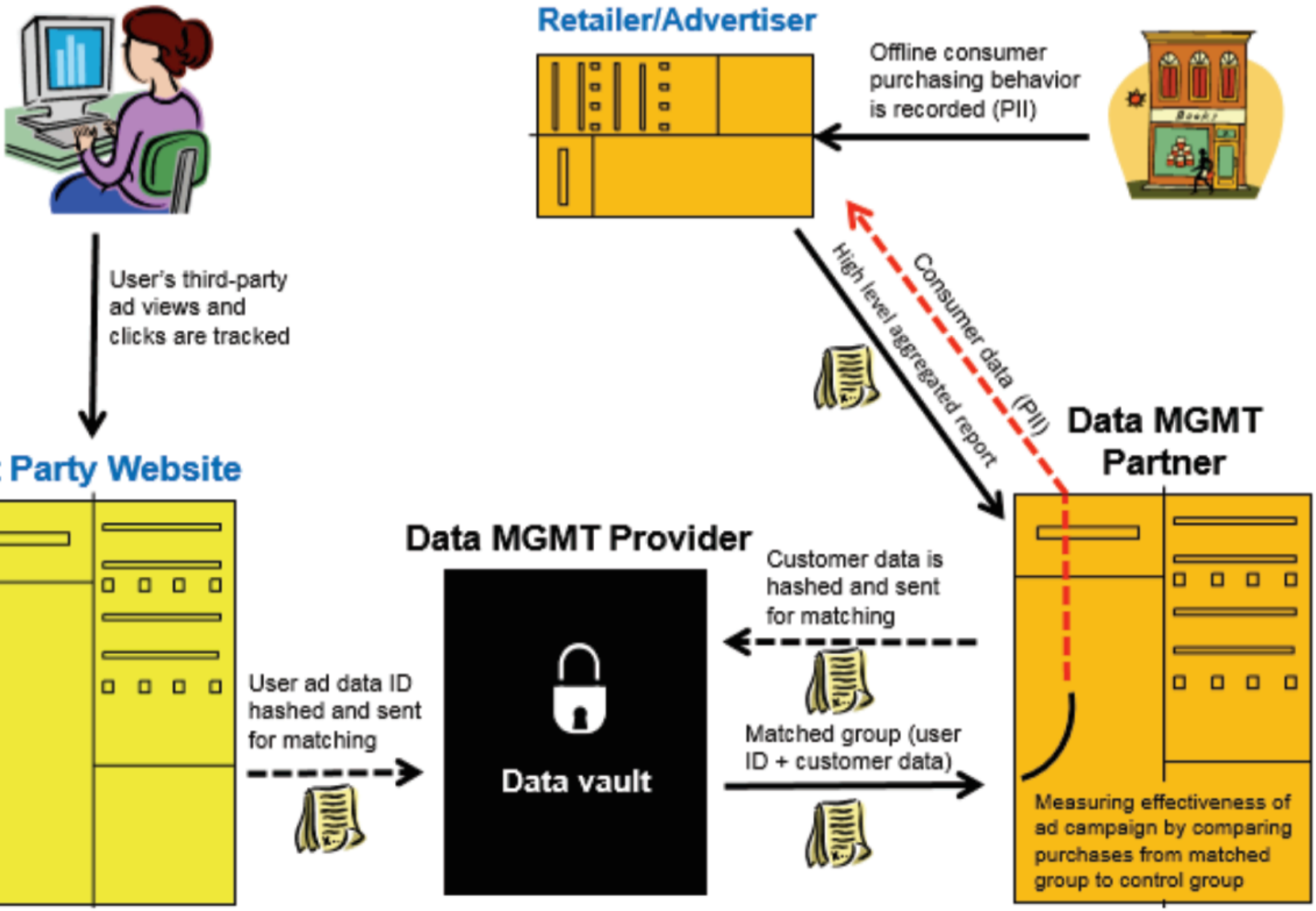
raditional Cookie Model

ings of data stored by browser & requested by servers when a user visits a website
- Includes a maximum expiration time
- User can clear the data at any time (all or some)



FUTURE OF PRIVACY FORUM

nderstanding Ad Effectiveness



umbling Cookies

ookie is **increasingly ineffective** because:

Cookies can only identify a user within the same browser

ncreasing % of browsing is on **mobile** browsers (Safari by default blocks third-party ookies)

ncreasing % of web behavior occurs in **apps. No link to cookies/web browsing.**

Consumers today access the web **via an expanding array of devices and platforms:**

Devices

- Phones
- PCs
- Tablets/eReaders
- Media Streaming / Gaming
- Wearables
- Virtual Reality
- Home Control

Consumer Software

- Search Engines
- Location Services
- Speech Recognition
- Office Suites
- Email Services
- Mobile Messaging
- Social Networks
- Cloud Services
- Photos
- Video / Music Players

Platforms

- Operating Systems
- Browsers
- App Stores
- Ad Networks
- Social Plug-Ins
- Analytics

FUTURE OF PRIVACY FORUM

. Authenticated Services

- Tracking across ISPs
- Notice via privacy policies
- Opt-out through provider

. Data Matching Across Websites & Apps

Third-Party Data

Data Matching Partner

Hashed Email + Cookie ID

Hashed Email Matched

Cookie ID

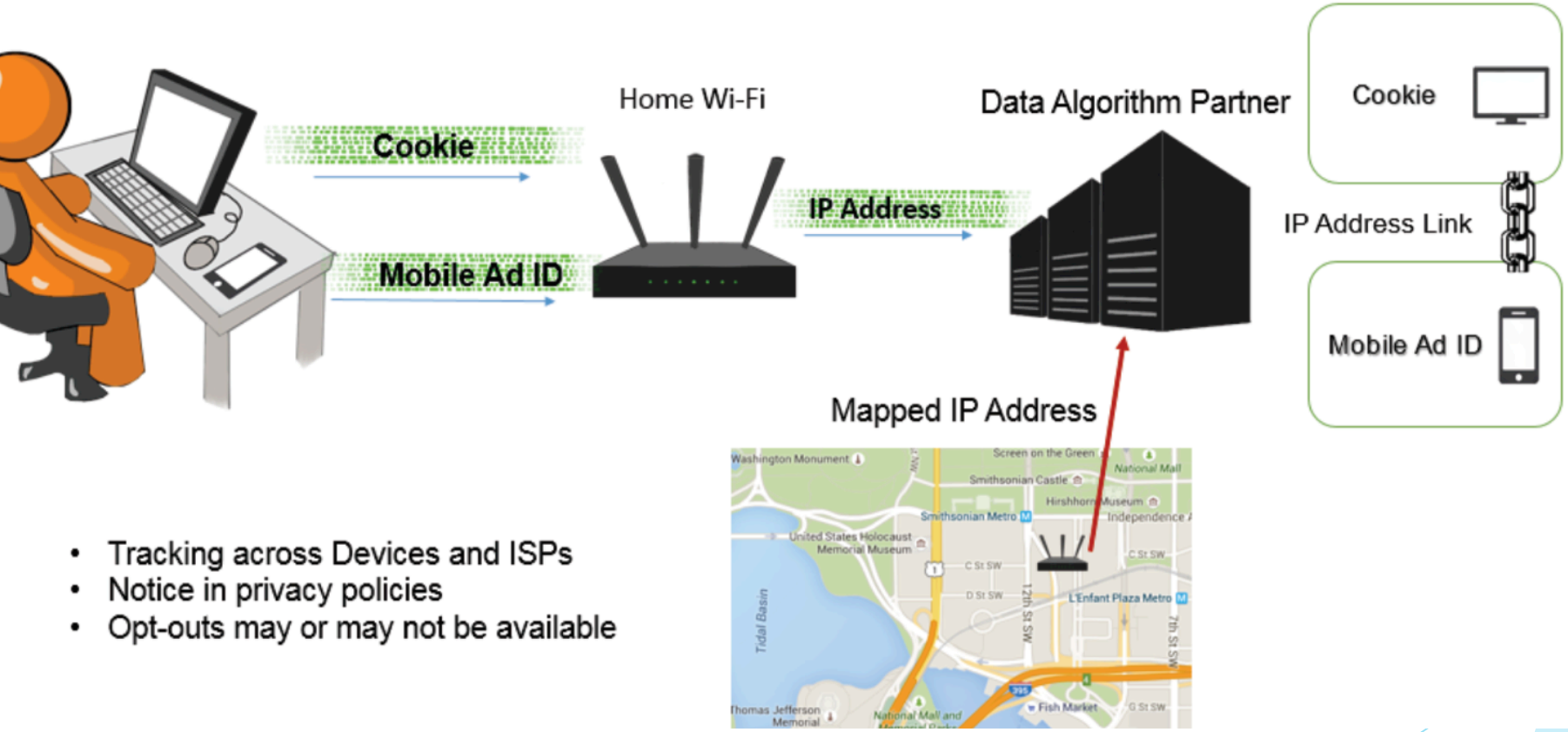
Mobile Ad ID

Hashed Email + Mobile Ad ID

- Tracking across Devices and ISPs
- Notice in privacy policies
- Opt-out options may or may not be available

Wi-Fi (IP Address or Local Router BBSSID)

tiple devices probably belong to the same owner if they access the Internet via the
ne home Wi-Fi router, and are turned on at roughly the same time every evening.



- Tracking across Devices and ISPs
- Notice in privacy policies
- Opt-outs may or may not be available

FUTURE OF PRIVACY FORUM

(Not necessarily limited by rotating IP addresses)

. Browser Fingerprinting

wsers and devices, even when they don't have an available cookie or advertising ID, nevertheless e unique attributes that allow the creation of a statistical identifier or a browser "fingerprint". o called "server side recognition" also enables the linkage of a user of a mobile app to the he user of a mobile web browser within the same device.

Browser Fingerprinting

ndustry terminology: Probabilistic geting, server side tracking or device cognition

rowser is queried for its agent ing, screen color depth, language, talled plugins with supported mime es, timezone offset and other abilities, such as local storage and ssion storage.

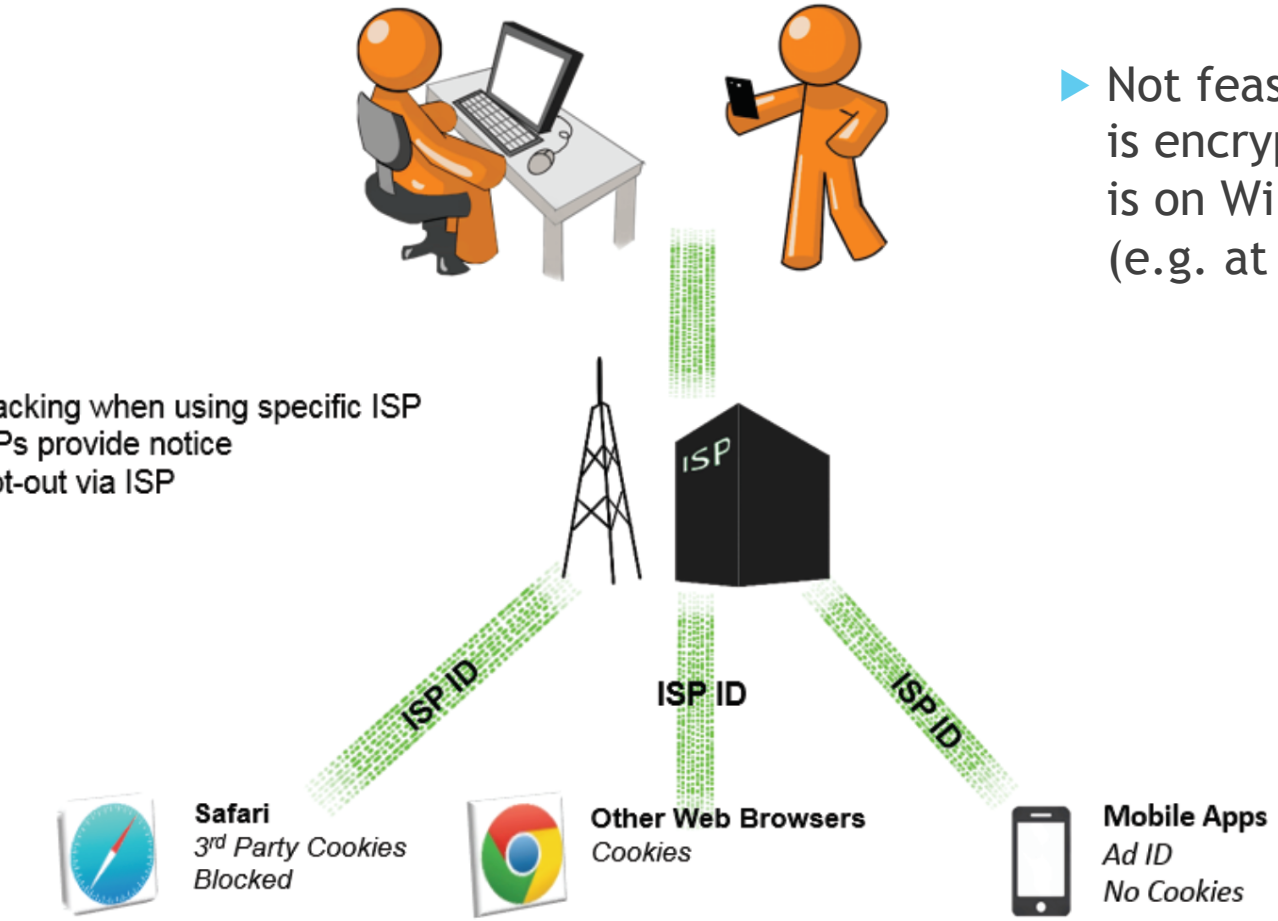
8 bits of entropy, meaning that only e in 286,777 other browsers will are its fingerprint.

or mobile, time differential latency o used.

```
navigator.userAgent // "Mozilla/5.0 (X11; Linux i686)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/27.0.1453.110 Safari/537.36"

navigator.language // "en-US"

var plugins = $.map(navigator.plugins, function(p){ var
mimeTypes = $.map(p, function(mimeType){ return
[mimeType.type, mimeType.suffixes].join("~"); }).join(","); return
[p.name, p.description, mimeTypes].join("::"); }); $.each(plugins,
function(i, p){// truncate only for blog example if

(p.length > 80){ console.log(p.substring(0, 77) + "..."); } else{
console.log(p); } }); /* Shockwave Flash::Shockwave Flash 11.7
r700::application/x-shockwave-flash~swf,a...

Chrome Remote Desktop Viewer::... Widevine Content Decryption
Module::Enables Widevine

licenses for playback of ... Native Client::application/x-nacl~nexe
Chrome PDF Viewer::application/pdf~pdf,application/x-google-
chrome-print-prev... Google Talk Plugin Video Accelerator::Google
Talk Plugin Video Accelerator ver... Google Talk Plugin::Version:
4.0.1.0::application/googletalk~googletalk Google Talk Plugin
Video Renderer::Version: 4.0.1.0::application/o1d~o1d Shockwave
Flash::Shockwave Flash 11.2 r202::application/x-shockwave-
flash~swf,a... */ screen.colorDepth // 24 new
Date().getTimezoneOffset(); // -240 !!window.localStorage //
true !!

window.sessionStorage // true
```

. ISPs

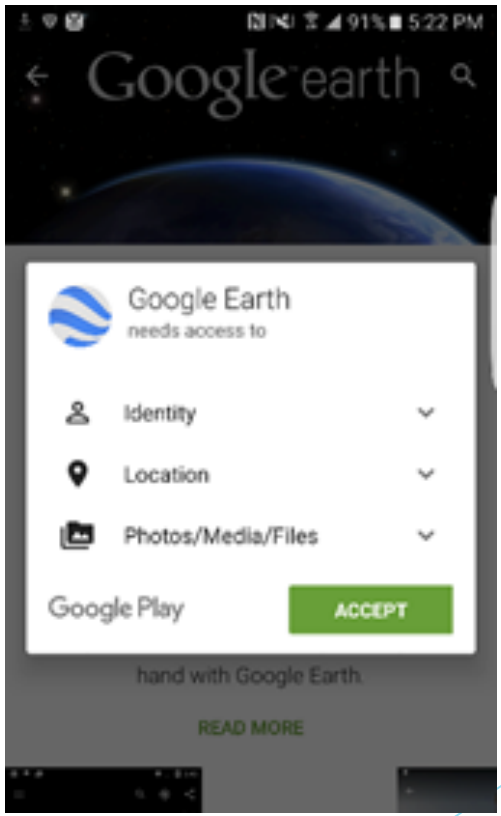
addition, Internet Service Providers (ISPs) can enable tracking of users across vices by inserting a unique identifier in web traffic that can be used by an ad work partner as a cookie alternative.



- Not feasible when web traffic is encrypted, or when the user is on Wi-Fi or using another ISP (e.g. at home vs. at work).

ocation Services

- Controlled by mobile operating system (OS)
- Aggregates data from different sources—including GPS, cellular triangulation, nearby Wi-Fi, and Bluetooth
- Apps/websites must get affirmative permission from the user via the OS to access

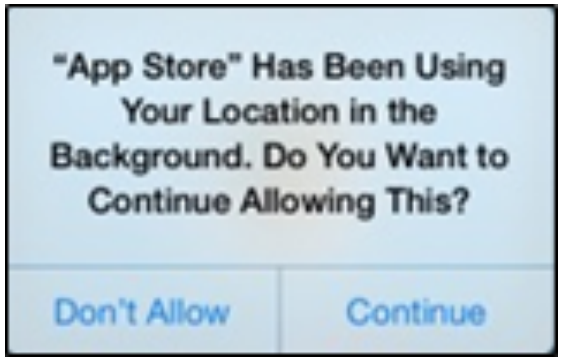


FUTURE OF PRIVACY FORUM

ocation Services

creasingly Nuanced Choices:

- In current iOS, location permission is separated into categories of "**Never**," "**While Using**," or "**Always**," with an arrow glyph indicating app usage.
- If an app has been using Location Services in the background (while the app was not in use), iOS will notify the user and re-confirm permission.
- iOS 10 will require apps/websites to state a **reason** why they are requesting the data
- Android will also move to a new permission model

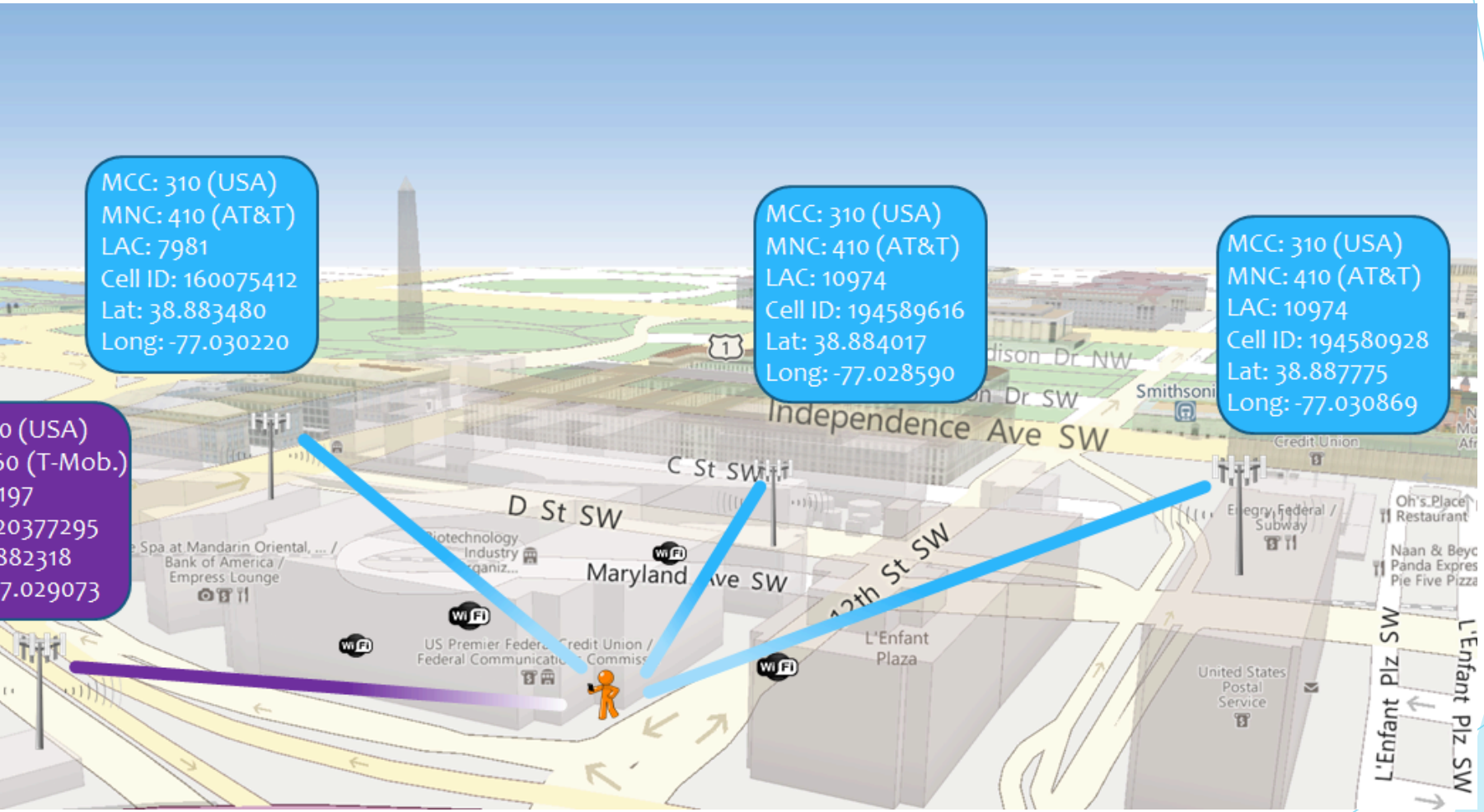


FUTURE OF PRIVACY FORUM

Other Mobile Location Methods

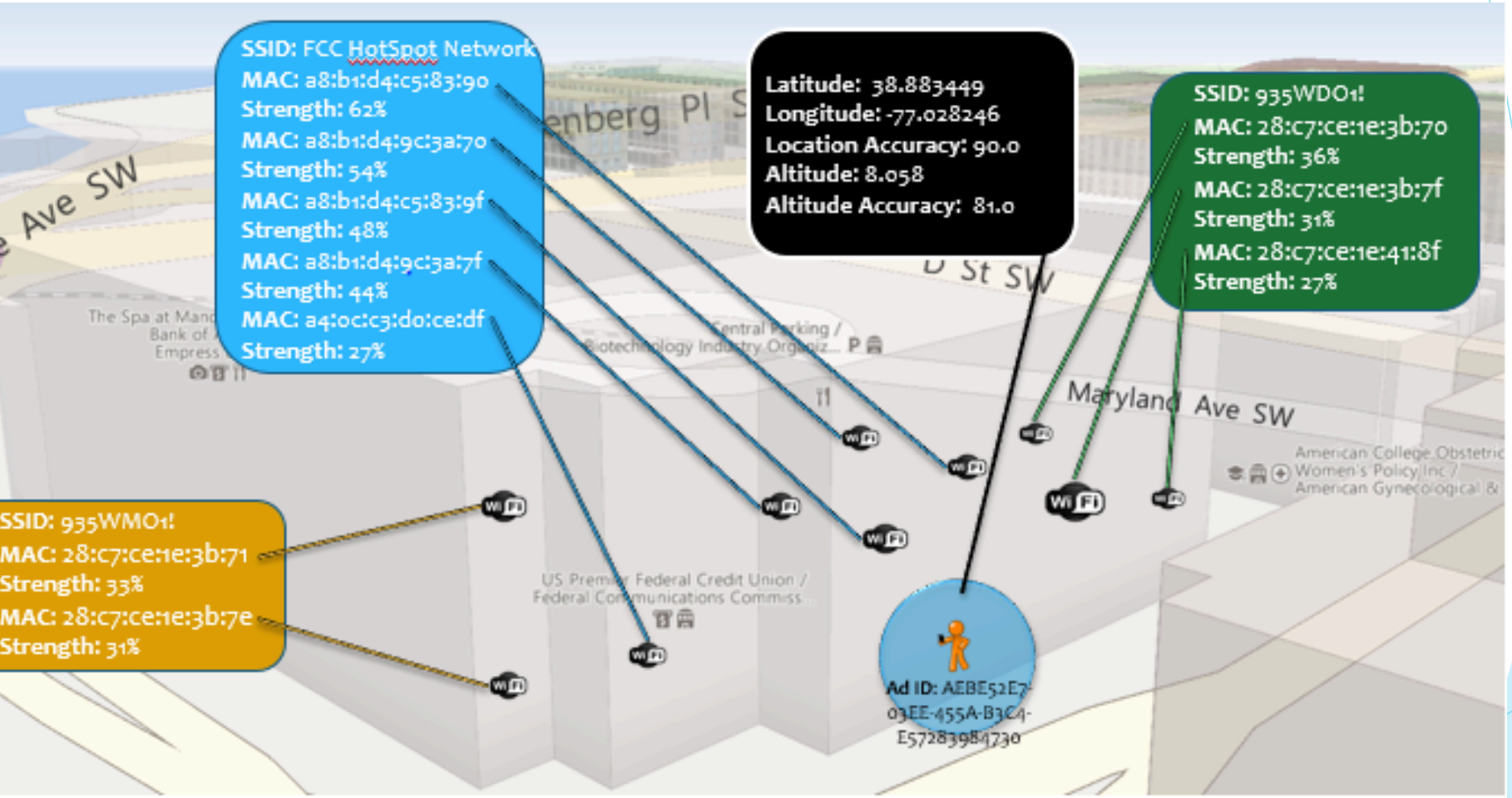
FUTURE OF PRIVACY FORUM

ell Tower Location (Coarse)



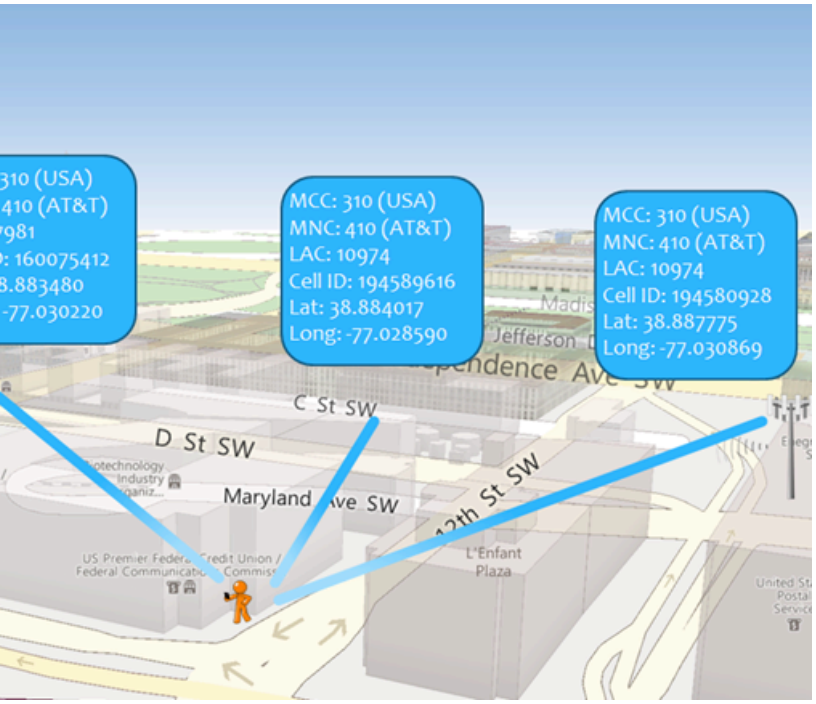
FUTURE OF PRIVACY FORUM

Wi-Fi Signals



FUTURE OF PRIVACY FORUM

arrier Triangulation



- Network-based location technique
- Available to Carriers
- Data also available to Apps and Websites without OS location permission through Cell ID lookup databases.
- Mobile OS location services are more accurate because supplemented by GPS and Wi-Fi.
  - Not available to Carriers. (Some additional information available via E911 channel.)

FUTURE OF PRIVACY FORUM

Wi-Fi Signals

- There are **databases** of all MAC addresses/ IP of Wi-Fi routers and their known locations
- All OS's + Android apps can detect router identifiers + their signal strengths without receiving location permission from user
- (Android permissions may be changing following the InMobi settlement)
- iOS apps cannot detect
- **Limited Opt Out choices for the owner of the router**

WPS	Unique Addresses	Opt Out?
Google	Unknown	_nomap
Microsoft	Unknown	Enroll MAC
Skyhook	Unknown	Enroll MAC IP
LocationAPI.org	> 709 million	_nomap
Mozilla	> 272 million	_nomap
Combain	> 602 million	_nomap
Navizon	> 480 million	No
WiGLE	> 198 million	Enroll MAC

FUTURE OF PRIVACY FORUM

essons from InMobi

- Ad network used data from Wi-Fi to infer location
- **Told its app developer partners** that when the user turned off Location Services, the network would stop collecting location information—but **collected location via Wi-Fi anyway,** even when user had turned **off** Loccation Services
- Federal Trade Commission (FTC) brought an enforcement action for **"deceptive practices"**

o what happens when there is a conflict between the ad net
arketer policy and the platform or browser policy or permiss
alogue?

Mobile Advertising Network InM
Settles FTC Charges It Tracked
Hundreds of Millions of Consum
Locations Without Permission

Company Will Pay $950,000 For Tracking Child
Without Parental Consent

FOR RELEASE

June 22, 2016

TAGS: Children's Online Privacy Protection Act (COPPA) | Technology | Mobile | Bureau of Consumer Protection | Consumer Protection | Privacy and Security | Children's Privac Consumer Privacy

Singapore-based mobile advertising company InMobi will pay $95 in civil penalties and implement a comprehensive privacy program settle Federal Trade Commission charges it deceptively tracked t locations of hundreds of millions of consumers – including childre without their knowledge or consent to serve them geo-targeted advertising.

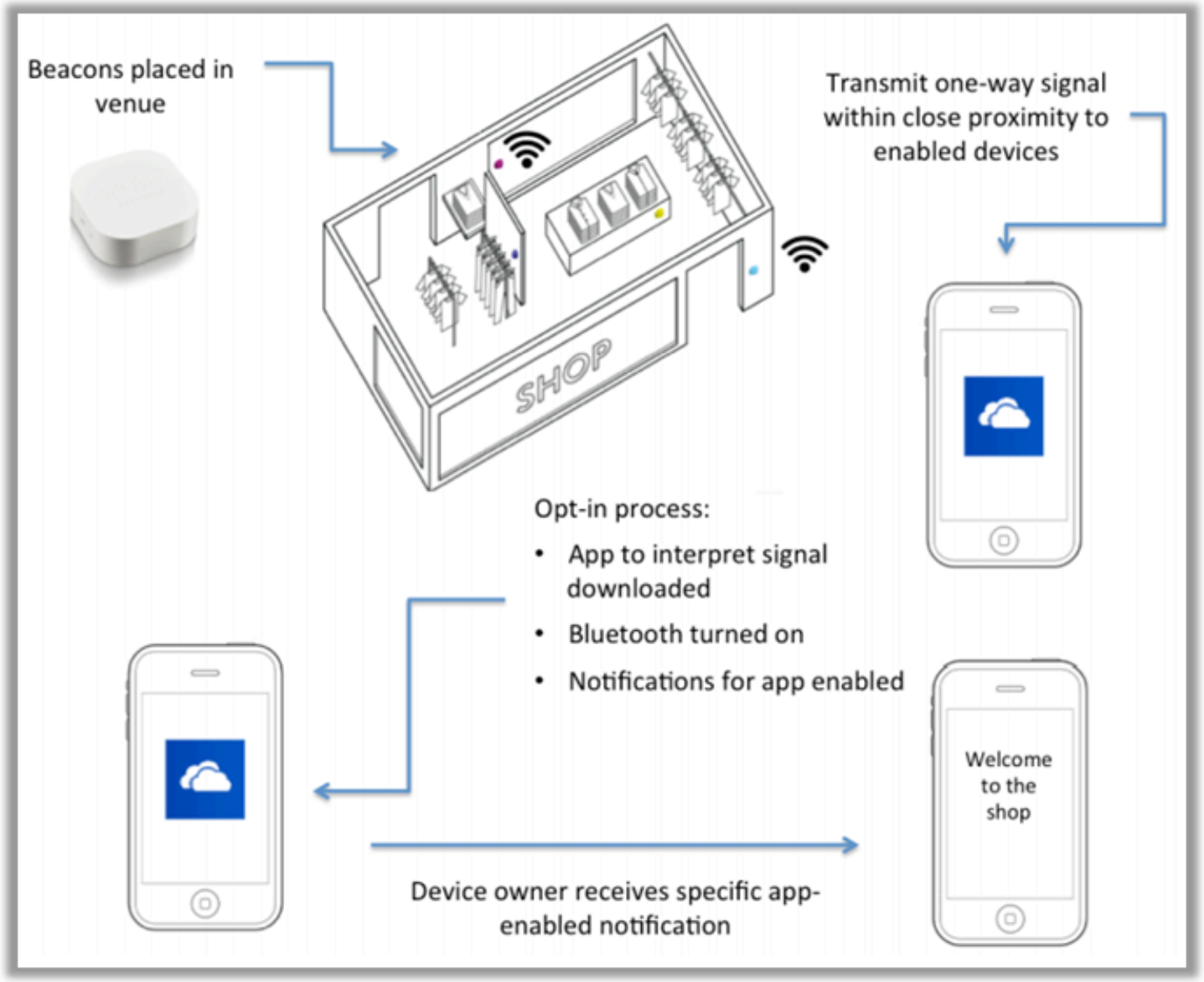
Press Release, June 22, 2016

FUTURE OF PRIVACY FORUM

eacons

- Consist of a chip and other electronic components (e.g., antenna) on a small circuit board.
- Essentially a radio transmitter that sends out a one-way signal to devices equipped to receive it.
- For more, see FPF's Understanding Beacons: A Guide to Beacon Technology

FUTURE OF PRIVACY FORUM

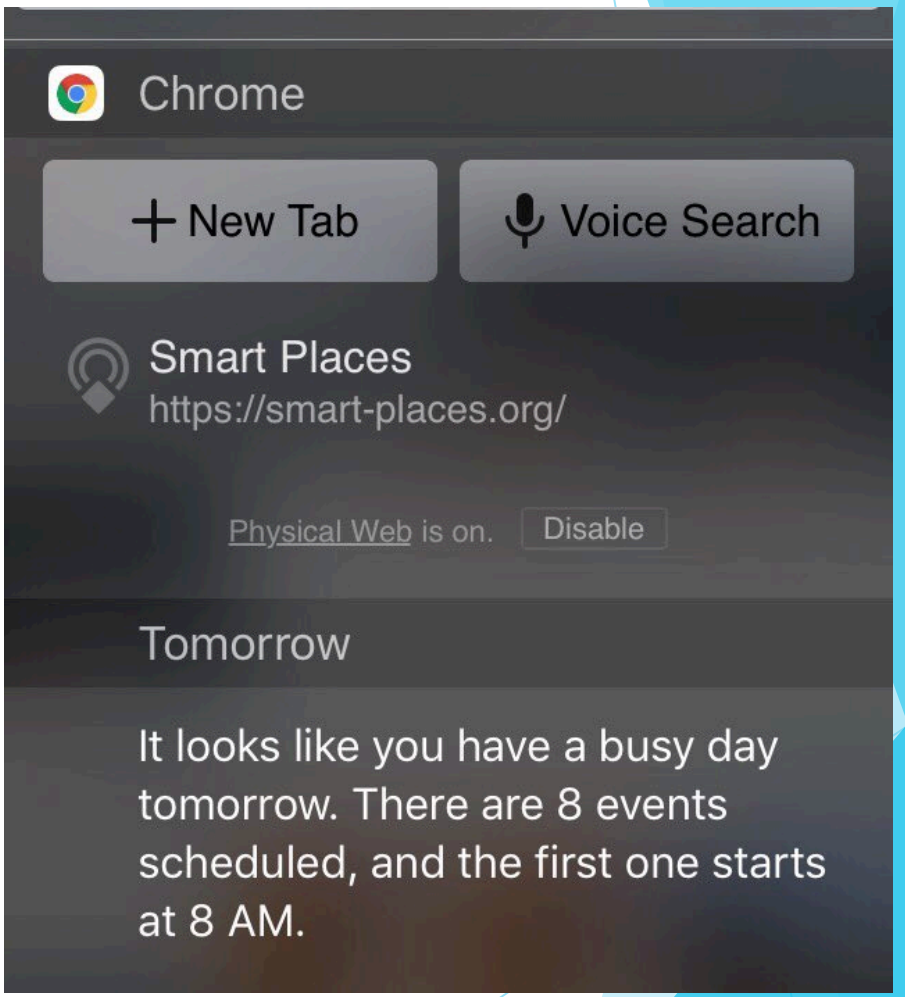


FUTURE OF PRIVACY FORUM

eacons

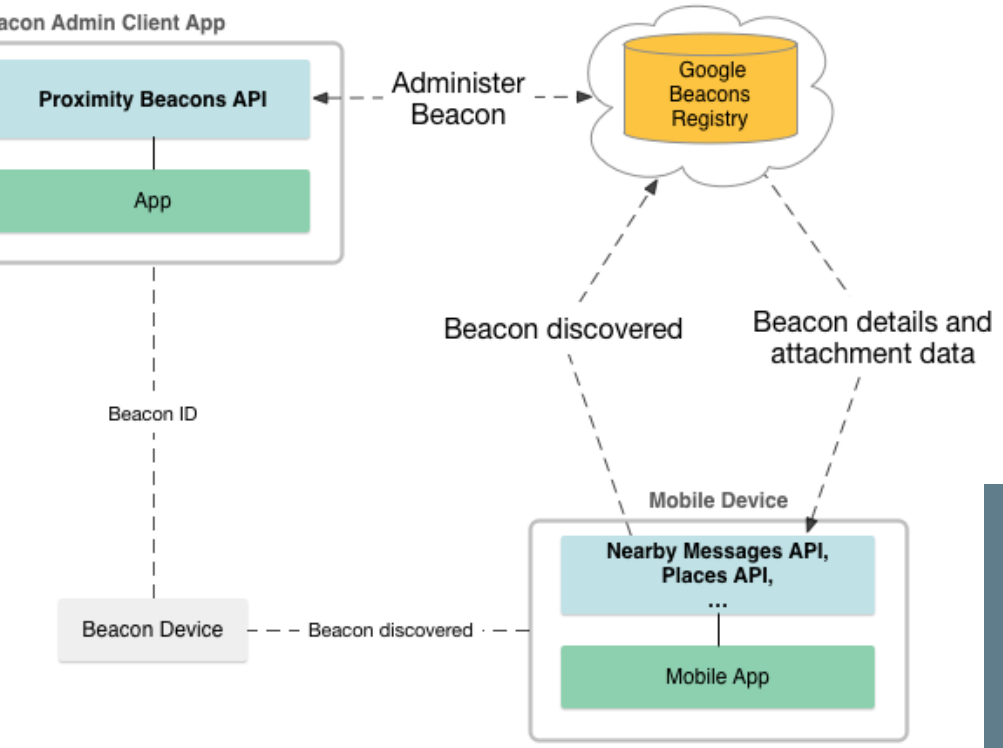
ving beyond apps…
ogle's Eddystone & the "Physical Web"

- Beacons can now trigger OS-level notifications and permit actions (such as clicking on a link or launching an app)
- User must enable The Physical Web, directly on Android or via Chrome on iOS

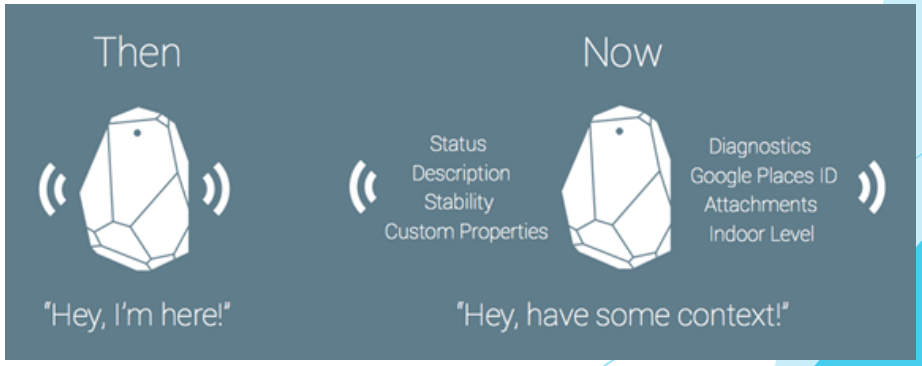


FUTURE OF PRIVACY FORUM

luetooth Beacons without App



- Google's Eddystone technology allows beacon owners to register the beacon location for improving location accuracy



FUTURE OF PRIVACY FORUM

Emerging Alternatives

- LED
- Audio
- Magnetic

FUTURE OF PRIVACY FORUM

rray of Mobile Sensors

Requires permission:

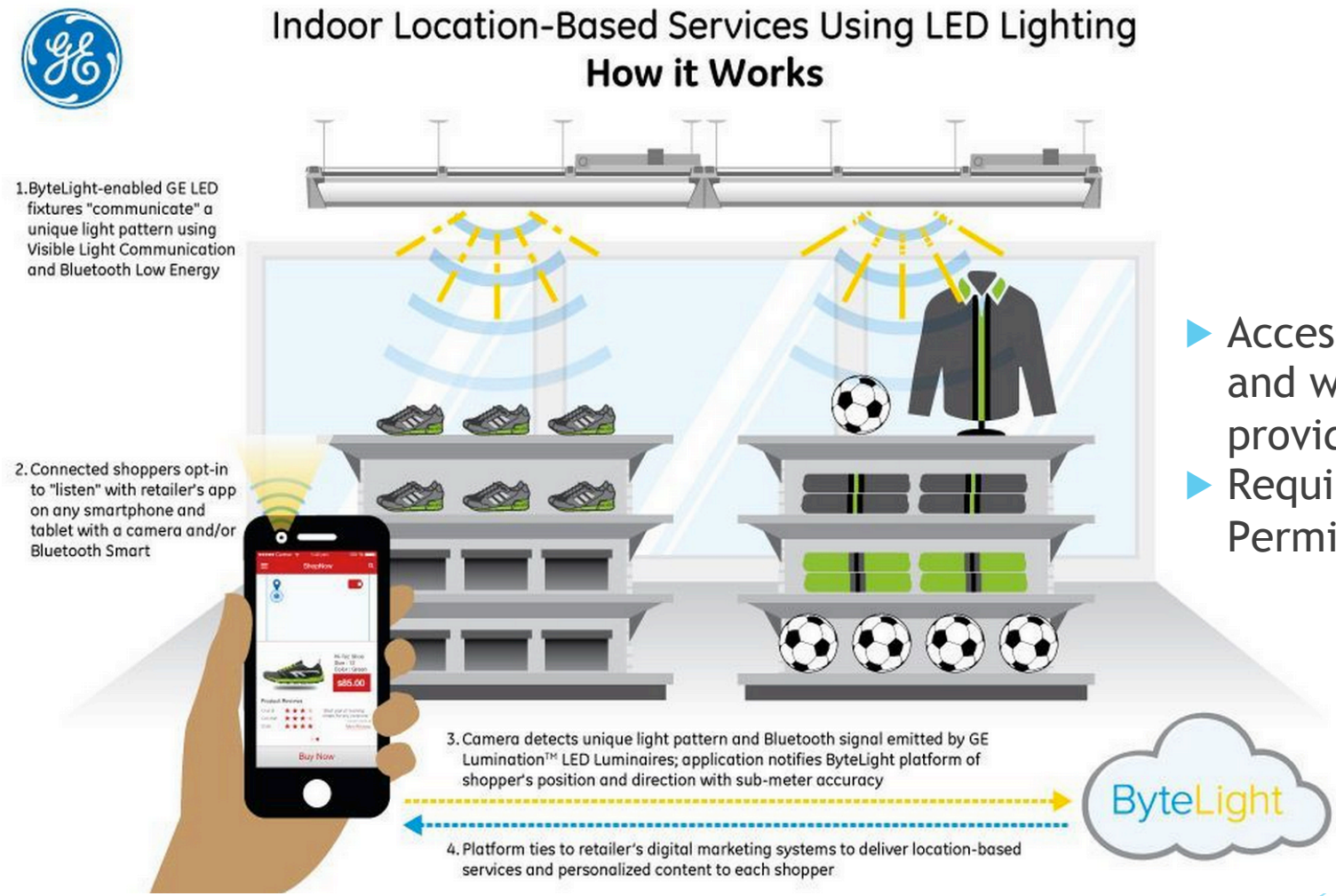
- Camera
- Microphone

No permission needed:

- Magnetometer
- Gyroscope
- Accelerometer

FUTURE OF PRIVACY FORUM

ED



- Accessible by App and website provider
- Requires Camera Permission

FUTURE OF PRIVACY FORUM

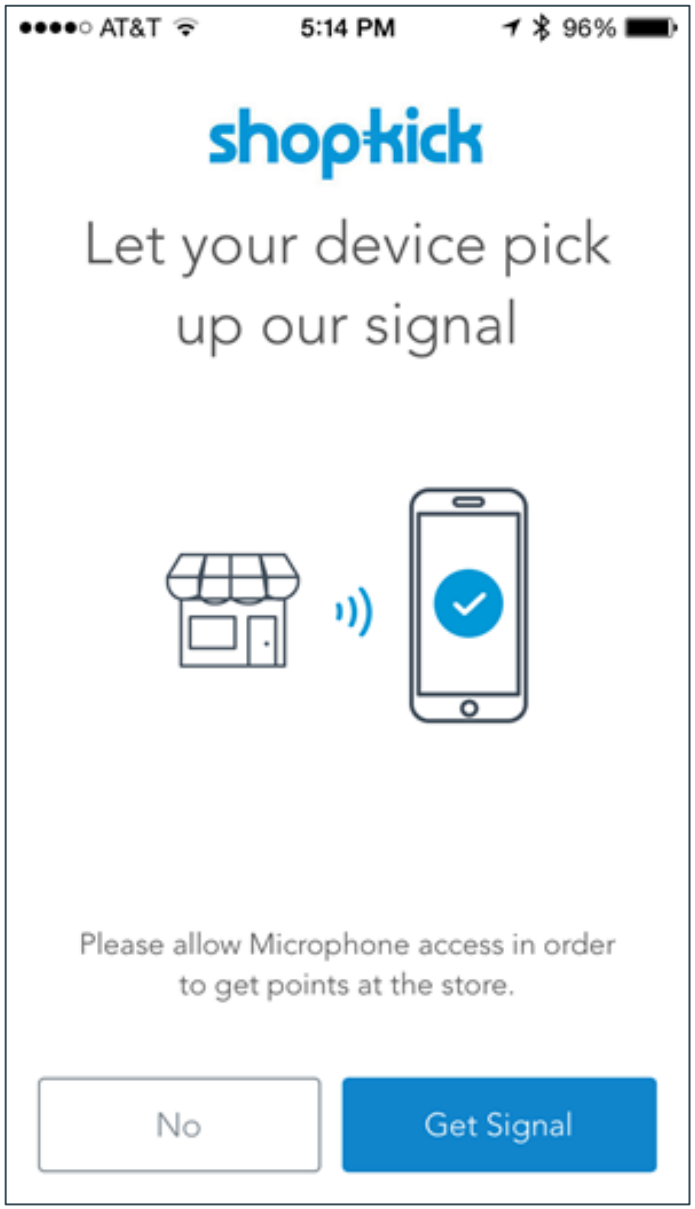
ED

- LED Lighting can be used for indoor positioning:
  - To locate people, help them locate items, measure dwell times
  - often combined with Bluetooth, Wi-Fi, and other sensors
- **Requires an app, with opt-in camera access**
- **Pros**: extremely precise (centimeters)
- **Cons**: app must be open **and** in the foreground due to OS limitation (thus often helpful to combine this with other signals, e.g. accelerometer/GPS); may require expensive front-end installation of lighting

FUTURE OF PRIVACY FORUM

udio

- **Requires app with microphone permission**
- App detects audio signal emitted by in-store device, inaudible to the human ear



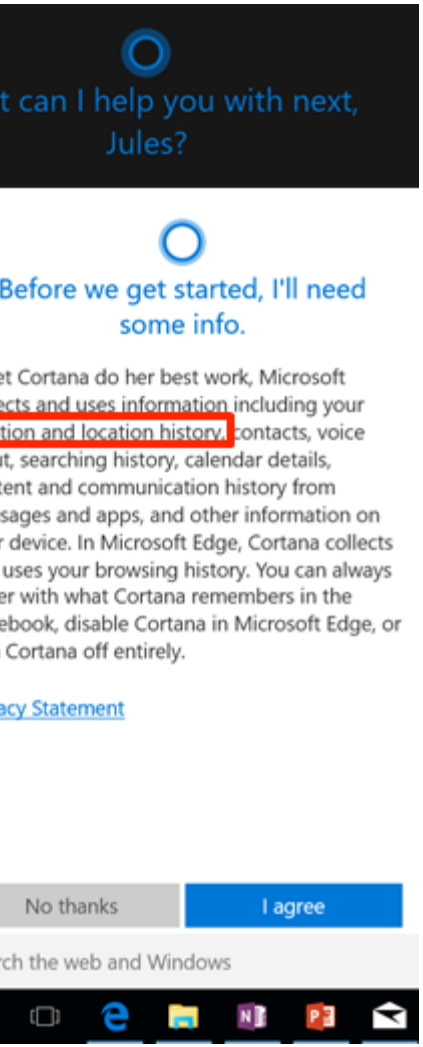
FUTURE OF PRIVACY FORUM

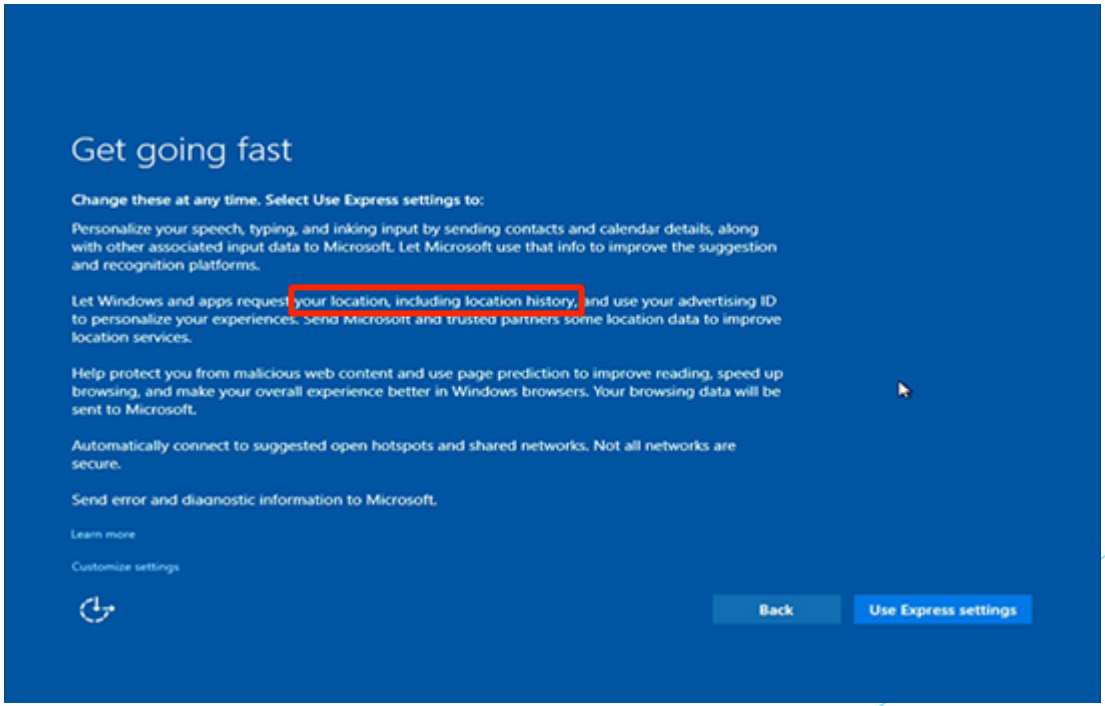
agnetic

- Wi-Fi Simultaneous Localization And Mapping, acquired by Apple, 2013.
- Uses device's magnetometer, gyroscope, and accelerometer with Wi-Fi-based position to improve accuracy
- Location accessible by OS and App provider
- No permissions needed
- **Requires prior mapping** of indoor area with similar device

FUTURE OF PRIVACY FORUM

Cs Tracked, too…





obile Location Analytics

- Network-based technique
- Available to brick-and-mortar businesses and 3rd-party partners
- Rotating mobile-device MAC address limits tracking
  - Currently on iPhone/iOS devices only
  - IEEE is developing a rotating-identifier standard

FUTURE OF PRIVACY FORUM

obile Location Analytics Opt Out

es such as airports, stores and hotels use Mobile Location Analytics (MLA) technology to understand the patterns of people in their venues. By learning and using insights, such as how long customers stand in d how they generally move around an area, these facilities can enhance operational efficiency and e user experience.

MLA technologies operate by detecting your device's WiFi MAC address or Bluetooth address – a 12 digit of letters and numbers assigned to your device by its manufacturers. You can enter your MAC address at e to opt out of the use of your MAC address for these programs by participating companies. Enter **both** iFi and Bluetooth MAC addresses to ensure the opt-out is effective across all participating companies. g off your device's WiFi or Bluetooth will also prevent your MAC address from being detected.

s running Apple iOS 8 automatically generate random WiFi MAC addresses, instead of broadcasting a consistent one (except when users oined a particular network or certain other times). As a result, for iOS 8 users, tracking is limited in those circumstances and the WiFi opt-out is .

earn more >>

ke me to the opt out >>

FUTURE OF PRIVACY FORUM

www.smart-places.org

ccuracy

- GPS via Satellites ~ 20 yards
- Cell Tower ~ varies depending upon density of towers (~50 yards-miles)
- Mobile OS Location Services using Wi-Fi and Bluetooth ~ 50-100 yards
- Location analytics: passively tracking MAC addresses ~ 10 yards
  - Mobile Location Code of Conduct (www.smart-places.org)
- Tracking location of users who have joined in-store Wi-Fi networks ~ 10 yards
- Beacon technologies ~ 1-2 yards
- Internal Magnetic Sensor ~ 1-2 yards

FUTURE OF PRIVACY FORUM

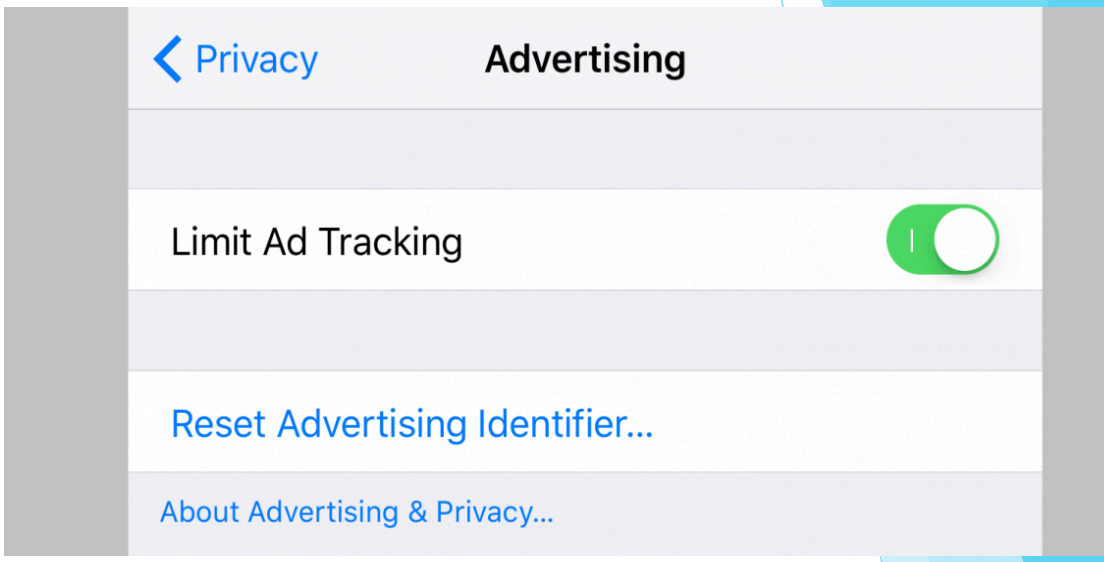
S 10 Changes

ted Ad Tracking

allows developers to target advertisements to app s by using a unique ID called **"Identifier for ertising" (IDFA or IFA).**

iously, users could select "Limit Ad king" (LAT) and a flag would be sent with the ad est--most treated this as an opt out of viorally targeted advertising (OBA).

S 10, LAT will zero out the IDFA. This will ent the previously permitted "frequency capping, bution, conversion events, estimating the number nique users, advertising fraud detection, and gging" uses of this ID.



Important

In iOS 10.0 and later, the value of `advertisingIdentifier` is all zeroes w the user has limited ad tracking.

FUTURE OF PRIVACY FORUM

hallenges

- What is Personal vs De-Identified
- What Is Sensitive
- Enter the Civil Rights Community
- Ethics – Review processes
- Algorithmic Discrimination
- Fairness
- Privacy in the Trump-Brexit Era

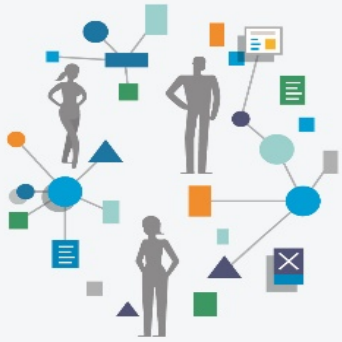
FUTURE OF PRIVACY FORUM

UAL GUIDE TO PRACTICAL DATA DE-IDENTIFICATION

Produced by FUTURE OF PRIVACY FORUM FPF.ORG

entists, regulators
mean when they
e-identification?
nonymous data
oseudonymous
fied information?
iability is not
lies on a
ith multiple
dentifiability.

mer on how
sh different
of data.



DEGREES OF IDENTIFIABILITY

Information containing direct and indirect identifiers.

PSEUDONYMOUS DATA

Information from which direct identifiers have been eliminated or transformed, but indirect identifiers remain intact.

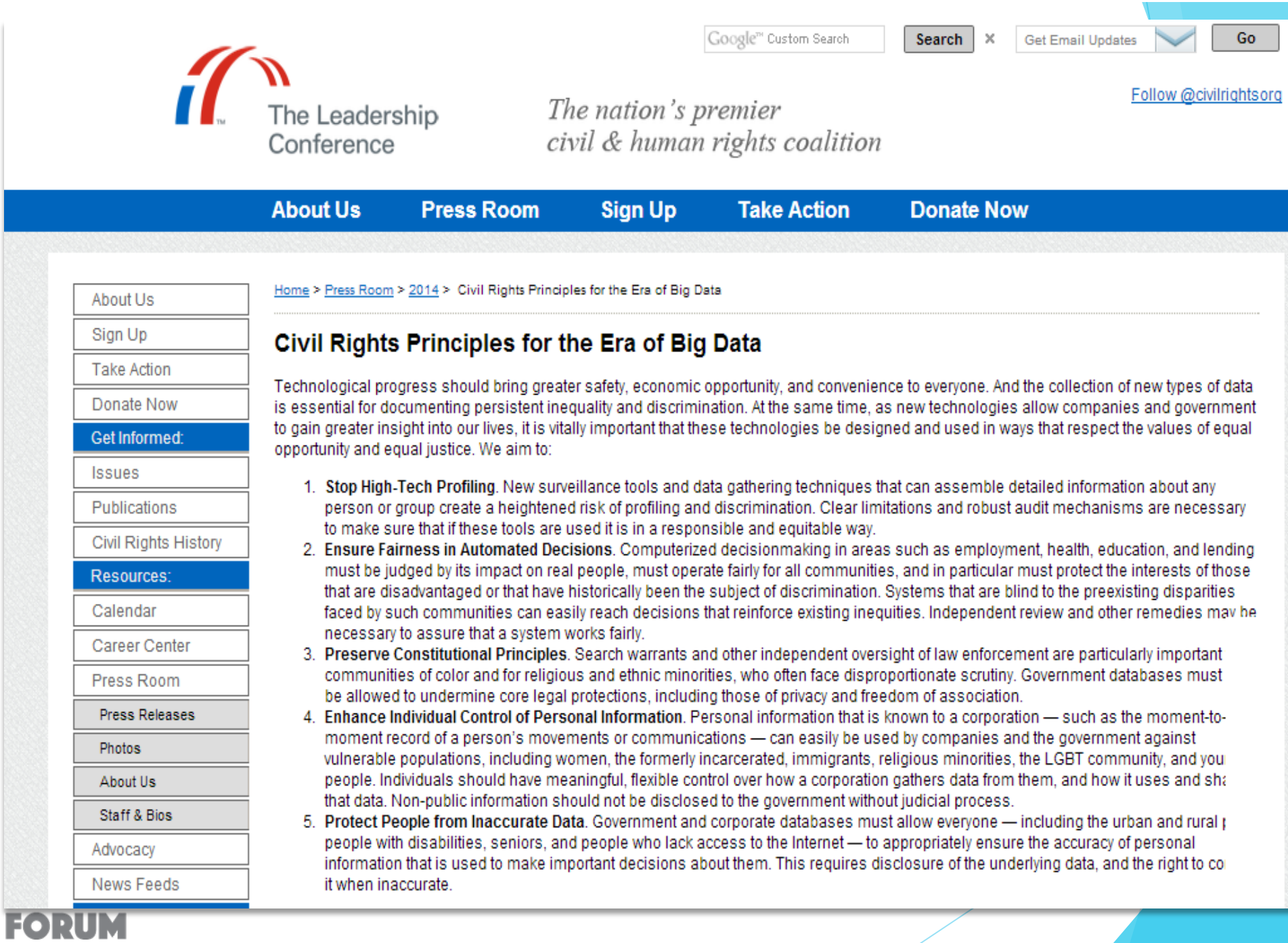
DE-IDENTIFIED DATA

Direct and known indirect identifiers have been removed or manipulated to break the linkage to real world identities.

ANONYMOUS D

Direct and indirect iden
been removed or manip
with mathematical and
guarantees to prevent r

	EXPLICITLY PERSONAL	POTENTIALLY IDENTIFIABLE	NOT READILY IDENTIFIABLE	KEY CODED	PSEUDONYMOUS	PROTECTED PSEUDONYMOUS	DE-IDENTIFIED	PROTECTED DE-IDENTIFIED	ANONYMOUS	A A
CT IDENTIFIERS that identifies a on without additional mation or by linking formation in the public ain (e.g., name, SSN)	INTACT	PARTIALLY MASKED	PARTIALLY MASKED	ELIMINATED or TRANSFORMED	ELIMINATED or TRANSFORMED	ELIMINATED or TRANSFORMED	ELIMINATED or TRANSFORMED	ELIMINATED or TRANSFORMED	ELIMINATED or TRANSFORMED	
RECT IDENTIFIERS that identifies an idual indirectly. Helps ect pieces of information an individual can be ed out (e.g., DOB, gender)	INTACT	INTACT	INTACT	INTACT	INTACT	INTACT	ELIMINATED or TRANSFORMED	ELIMINATED or TRANSFORMED	ELIMINATED or TRANSFORMED	
GUARDS and CONTROLS nical, organizational egal controls preventing oyees, researchers or third parties from entifying individuals	NOT RELEVANT due to nature of data	LIMITED or NONE IN PLACE	CONTROLS IN PLACE	CONTROLS IN PLACE	LIMITED or NONE IN PLACE	CONTROLS IN PLACE	LIMITED or NONE IN PLACE	CONTROLS IN PLACE	NOT RELEVANT due to nature of data	
SELECTED EXAMPLES	Name, address, phone number, SSN, government-issued ID (e.g., Jane Smith, 123 Main Street, 555-555-5555)	Unique device ID, license plate, medical record number, cookie, IP address (e.g., MAC address 68:A8:6D:35:65:03)	Same as Potentially Identifiable except data are also protected by safeguards and controls (e.g., hashed MAC addresses & legal representations)	Clinical or research datasets where only curator retains key (e.g., Jane Smith, diabetes, HgB 15.1 g/dl = Csrk123)	Unique, artificial pseudonyms replace direct identifiers (e.g., HIPAA Limited Datasets, John Doe = 5L7T LX619Z) (unique sequence not used anywhere else)	Same as Pseudonymous, except data are also protected by safeguards and controls	Data are suppressed, generalized, perturbed, swapped, etc. (e.g., GPA: 3.2 = 3.0-3.5, gender: female = gender: male)	Same as De-Identified, except data are also protected by safeguards and controls	For example, noise is calibrated to a data set to hide whether an individual is present or not (differential privacy)	Very data data pop 52.6 DC r



Google™ Custom Search Search × Get Email Updates Go

The Leadership Conference

The nation's premier civil & human rights coalition

Follow @civilrightsorg

About Us **Press Room** **Sign Up** **Take Action** **Donate Now**

About Us
Sign Up
Take Action
Donate Now
Get Informed:
Issues
Publications
Civil Rights History
Resources:
Calendar
Career Center
Press Room
Press Releases
Photos
About Us
Staff & Bios
Advocacy
News Feeds

Home > Press Room > 2014 > Civil Rights Principles for the Era of Big Data

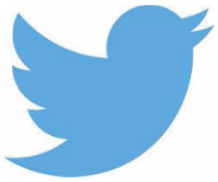
Civil Rights Principles for the Era of Big Data

Technological progress should bring greater safety, economic opportunity, and convenience to everyone. And the collection of new types of data is essential for documenting persistent inequality and discrimination. At the same time, as new technologies allow companies and government to gain greater insight into our lives, it is vitally important that these technologies be designed and used in ways that respect the values of equal opportunity and equal justice. We aim to:

1. **Stop High-Tech Profiling**. New surveillance tools and data gathering techniques that can assemble detailed information about any person or group create a heightened risk of profiling and discrimination. Clear limitations and robust audit mechanisms are necessary to make sure that if these tools are used it is in a responsible and equitable way.
2. **Ensure Fairness in Automated Decisions**. Computerized decisionmaking in areas such as employment, health, education, and lending must be judged by its impact on real people, must operate fairly for all communities, and in particular must protect the interests of those that are disadvantaged or that have historically been the subject of discrimination. Systems that are blind to the preexisting disparities faced by such communities can easily reach decisions that reinforce existing inequities. Independent review and other remedies may be necessary to assure that a system works fairly.
3. **Preserve Constitutional Principles**. Search warrants and other independent oversight of law enforcement are particularly important communities of color and for religious and ethnic minorities, who often face disproportionate scrutiny. Government databases must be allowed to undermine core legal protections, including those of privacy and freedom of association.
4. **Enhance Individual Control of Personal Information**. Personal information that is known to a corporation — such as the moment-to-moment record of a person's movements or communications — can easily be used by companies and the government against vulnerable populations, including women, the formerly incarcerated, immigrants, religious minorities, the LGBT community, and you people. Individuals should have meaningful, flexible control over how a corporation gathers data from them, and how it uses and sha that data. Non-public information should not be disclosed to the government without judicial process.
5. **Protect People from Inaccurate Data**. Government and corporate databases must allow everyone — including the urban and rural p people with disabilities, seniors, and people who lack access to the Internet — to appropriately ensure the accuracy of personal information that is used to make important decisions about them. This requires disclosure of the underlying data, and the right to co it when inaccurate.

FORUM

Questions?



- www.fpf.org
- facebook.com/futureofprivacy
- @futureofprivacy

FUTURE OF PRIVACY FORUM