Geolocation Tracking and Privacy

Paige Boshell, Managing Member, Privacy Counsel LLC, Birmingham, AL

We will discuss tracking technologies, recent scandals, relevant legal and industry guidance, consent difficulties, and ethical considerations. This talk will focus on physical location (as opposed to online tracking) of the consumer.
THE POWER OF PLACE

Privacy and Location Data
American Bar Association
Cyberspace Law Institute & Winter Working Meeting
January 26, 2019
AGENDA

Geolocation = physical (versus online) location

Methods of collection of data

Uses of data

Consumer awareness and consent

Legal requirements and industry guidance

Ethical and extra-legal considerations
WHO WANTS TO KNOW WHERE YOU ARE RIGHT NOW

Your mother
Weather apps
Google
Nick Jonas
Local PD
LOCATION DATA – KEY CONCEPTS

Location: latitude, longitude, altitude, timing, frequency, precision, accuracy

Digital map or geobase: database of objects used to pinpoint other objects
Can layer by cluster or individual

An individual cannot be in more than one place at a time → PLACE as identifier

HOW:
Collector – GNSS (satellite), GPS, cell towers, wi-fi, beacons, audio/LED
Individual – device/app
Interactivity
LOCATION TRACKING DEVICES

Premise: devices track your location in order to provide products or services to you
LOCATION TRACKING – MOBILE APPS

Find your way
Find your friends
Find your stuff
Find your weather
Find what is near you
Be found

Same premise: apps track your location in order to provide products or services to you
LOCATION TRACKING IN THE NEWS

Connected Car Technology Can Enable Abusers to Track Their Victims

A growing number of automakers are enabling location tracking in internet-connected cars, a technology that experts say can be misused by abusers to track their victims.

By Tracey Lindeman | Aug 14 2018

Implications of tech not fully-realized
LOCATION DATA – USE CASES

*Business:*
- Logistics, planning, and fleet control
- Supply-chain tracking, inventory control
- Customer experience
- Targeted advertising/marketing

*Governmental/Public:*
- Municipal planning
- Traffic management
- Disease tracking/control
- Air quality monitoring
LOCATION DATA - ANALYTICS

**Goal:** Improve efficiencies, volumes of scale, manage risk, deploy new services, measure performance, anticipate needs

*Aggregate* individual geocodes with larger, fixed geographical data points

*Correlate* repeating clusters – crime, tornadoes, voters, purchases

*Apply* metrics – efficiency, value, safety, risk

**Challenges:** large volume, batch versus real-time, stored across systems, relationship to business operations, proprietary data
LOCATION DATA—DATA POINTS OR ITEMS

• **Traditional location units**: city, state, zip code, street or box address

• **Geolocation units**: longitude and latitude (geocodes), proximity to centralized device (cell tower, fitness tracker, beacons) or data points collected in real-time (by apps, web services, or IoT)

• **Structured data**: raw data organized into formatted repository so that elements may be readily used for processing and analysis

• **Data lakes**: enterprise system of all collected data in raw form (structured or unstructured) – storage

• **Data warehouses**: central repository of structured data integrated multiple sources – business analytics

Companies collect and store new more precise geolocation data in combination with more traditional locational units.
In the US, Big Data has viewed location data as property of the collector.

Companies collect and store new more precise geolocation data in combination with more traditional locational units.
LOCATION DATA – AGGREGATORS AND RESALE

Wireless carriers ➔ Aggregators ➔ Apps: Exact location identified to specific consumer

Purpose to allow apps to obtain their customer’s location to fulfill service to customer

Goal to provide consistent consumer experience across multiple carriers

Consent app access to location data subject to requirement of consumer consent

Reliance on consent plus NDA
LOCATION DATA – AGGREGATORS AND RESALE

Reporter paid bounty hunter $300
With the cell phone number alone, the bounty hunter was able to provide the reporter “a screenshot of Google Maps, containing a blue circle indicating the phone’s current location, approximate to a few hundred metres.”

1/8 Motherboard story breaks

1/10-1/16 Verizon, T-Mobile, AT&T, and Sprint announce plans to stop selling location data

1/11 House Energy & Commerce requests briefing by FCC

1/16 House Energy & Commerce sent letters to Zumigo, Microbilt, T-Mobile, AT&T, Sprint, and Verizon
LOCATION DATA – APP DEVELOPERS AND RESALE

Apps → Buyers: Exact location identified to unique identifier

*Purpose* to monetize location data on an aggregated basis

*Goal* to allow third parties to spot trends and patterns in consumer behavior (marketing, investment)

*The catch*: each identifier is unique and can be linked to an individual by combining location data with other data (such as name and address); raw data is still available to insiders and employees

Reliance on disclosure/consent and aggregation
LOCATION DATA –RESALE AND LAW ENFORCEMENT

Warrantless location tracking: Some law enforcement agencies purchase their own cell tracking tech or purchase data from apps and resellers

“The ACLU received over 5,700 pages of documents from roughly 250 local law enforcement agencies regarding cell phone tracking. The responses show that while cell phone tracking is routine, few agencies consistently obtain warrants. Importantly, however, some agencies do obtain warrants, showing that law enforcement agencies can protect Americans' privacy while also meeting law enforcement needs.”

The practice is so common that cell phone companies have manuals for police explaining what data the companies store, how much they charge police to access that data, and what officers need to do to get it.
LOCATION DATA – WEATHER APPS AS BIG DATA

The Weather Channel (IBM sub) tracked location data continuously and stored for years and sold it to third parties – LA sues for lack of consent (UDAP)

Accuweather and Weather Bug do this too

Chinese weather app also collects email addresses and IMEIs

Reliance on disclosure/consent
CONSUMER AWARENESS

64% use connected devices

40% aware of sharing with third parties

29% not aware of sharing

31% confident data not shared across devices*

Key takeaway: many consumers do not understand how their location data is used or shared

* F. Truta, “Expanded access to personal information raises privacy concerns with connected devices” (10/30/18)
https://www.bitdefender.com/box/blog/iot-news/expanded-access-personal-information.raises-privacy-concerns-connected-device
LOCATION TRACKING – CONSUMER CONFUSION

Every device and app collects and uses data differently

Choice fallacy: Always/never/while using (FTC actions, Google location history)

Premise: devices and apps track your location in order to provide products or services to you
“Mobile Privacy Disclosures: Building Trust Through Transparency”


FTC’s Privacy Report (2012) - Precise location data is considered sensitive (similar to children’s data, health, and financial information), and should not be stored beyond time needed for service provided. Affirmative express consent is generally required for collection, except when appropriate in context (e.g., for searching nearby).
RECENT FEDERAL TRADE COMMISSION ENFORCEMENT

UDAP: Federal Trade Commission Act § 5: “Unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful.”

Focus: deceptive privacy practices, unfair privacy practices

Resolution: 20-year privacy program

Key takeaways:
- Lack of disclosure, meaningful consent
- Conflict with stated privacy practices

Note: no substantive anti-location limits
RECENT FEDERAL TRADE COMMISSION ENFORCEMENT

**UBER Godview consent order (2017)** – real-time geolocation data tracked even when user not riding and broad access and misuse by employees

**BLU Products consent order (2018)** – privacy statements that info collected by unlocked Android devices only as needed to provide service and administrative, technical, and procedural procedures to protect info, Chinese security vendor to update devices collected geolocation info and other sensitive info

*Key takeaway: deceptive disclosure and unfair practices*
COPPA: Applies to the online collection of personal information by persons or entities under about children under 13 years of age and provides what a website operator must include in a privacy policy, when and how to seek verifiable consent from a parent, and what responsibilities an operator has to protect children’s privacy and safety online including restrictions on marketing to those under 13. 2013 compliance guide addresses location-based services.

2018 warning letters: GPS Gator Watch and Tinitell watch track geolocation data of children (parental tracker and geofencing services)

Key takeaway: lack of disclosure and verifiable parental consent
RECENT FEDERAL TRADE COMMISSION ENFORCEMENT

**COPPA and UDAP: 2016 InMobi consent order**

Location information of app users tracked, aggregated with wireless network data, inference of exact physical location of user to serve location-based ads (real-time, over time, clusters)

*Even when consumer opted out of collection, turned off location history or phone*

Over 1 billion users worldwide, including children

*Key takeaway: deceptive disclosure and opt-out and lack of verifiable parental consent*
RECENT FEDERAL TRADE COMMISSION ENFORCEMENT

Google investigation (2018)

2011 Consent Order – Buzz social network opt-out for Gmail users ineffective, privacy disclosures confusing: “Nah, go to my inbox” “Turn off Buzz”

Resolution: ban on privacy misrepresentations, 20-year privacy program with regular, independent audits

2012 Consent Order – placement of ad tracking cookie on Safari user computers deceptive due to representations that Safari blocking of cookies effective as opt-out from tracking and targeted advertising

2018 investigation - potential deceptive acts and practices used by Google to “track and commoditize American consumers” based on location history; Maps - cancel/ok; Bluetooth, demographic “inferences”
FEDERAL TRADE COMMISSION - LABMD

FTC consent order requirements are not rule-focused but tend to be risk-based, technology neutral, and reliant on evolving industry standards.

In LabMD, the Eleventh Circuit held that the FTC’s consent order against LabMD was void because the security program requirements in its cybersecurity consent order was not specific enough to be enforceable.

*The opinion calls into question the enforceability of existing FTC consent orders and the FTC’s ability to craft a concept of “reasonable security” – and therefore privacy - on a case-by-case basis.*
**Carpenter v. United States**

**Facts:** series of armed robberies
FBI SCA order for 4 months’ worth of suspect’s cell records, including cell-site location information (“CSLI”)
FBI “obtained 12,898 location points cataloging Carpenter’s movements—an average of 101 data points per day”, which led to arrest

**Reasoning:** expectation of privacy trumps third party doctrine; no invasion of privacy (property) required; “unique and pervasive nature of data”

**Issue:** whether CSLI was result of unreasonable search and seizure absent warrant based on probable cause (SCA order “specific and articulable facts showing that there are reasonable grounds to believe” the records “are relevant and material to an ongoing criminal investigation”)

**Holding:** CSLI obtained under SCA order constituted unreasonable search and seizure prohibited by 4th A- “an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through” cell-site location information
US SUPREME COURT: FOURTH AMENDMENT

Carpenter v. United States

Third-party doctrine – information voluntarily given to a third party is not covered by the 4\textsuperscript{th} A

*United States v. Miller* (1976) – bank records excluded
*Smith v. Maryland* (1979) – cell phone call records excluded

Mosaic theory – aggregation of location information covered by 4\textsuperscript{th} A

*Riley v. California* (2014) - 4\textsuperscript{th} A applies to cell phone data of arrested suspect
**US SUPREME COURT: FOURTH AMENDMENT**

_Carpenter v. United States_

Opinion declined to extend third party doctrine to CSLI

“[m]uch like GPS tracking of a vehicle, cell phone location information is detailed, encyclopedic, and effortlessly compiled”

“when Smith was decided in 1979, few could have imagined a society in which a phone goes wherever its owner goes, conveying to the wireless carrier not just dialed digits, but a detailed and comprehensive record of the person’s movements.”

Limits: shorter-term tracking, imminent threat/security
GENERAL DATA PROTECTION REGULATION (EU)

Location information not separately governed by GDPR

*Location information is considered “personal data” if it relates to an identifiable individual*
- Legitimate business purpose
- Consent (valid)

All requirements applicable to personal data apply, including restrictions on profiling and automated decision-making

*Focus: risk or harm to consumer*

Takeaway: consent will now be required in connection with most collection and use of location data
Google: Location tracking even when location history turned off

Multiple GDPR complaints across 7 countries:

Deceptive practices to get consumer to enable both Location History (default = off) and Web & App Activity (default = on)

-> No disclosure
-> No consent
AUTOMATIC LICENSE PLATE READERS/RECOGNITION

Photos v. digital

**State laws:**

*Primarily apply to law enforcement (CA private)*
*Restrictions on use, substantive limits on collection, retention, and use*
*Disclosure requirements*
CALIFORNIA LAW

ALPR (California Civil Code §§ 1798.90.5-1798.90.55, 1798.29, 1798.82)
Automobile "Black Boxes" - California Vehicle Code section 9951
California Electronic Communications Privacy Act (CalECPA) - Penal Code section 1546
Online Privacy Protection Act of 2003 - Online Privacy Protection Act of 2003 - California Business and Professions Code sections 22575-22579 (CALOPPA)
Electronic Toll Collection Systems - Streets and Highways Code sections 31490-31490
Electronic Surveillance in Rental Cars - California Civil Code section 1939.23
Fourth Amendment Protection Act - California Government Code section 7599
Identification Devices, Prohibition on Bodily Implanting - California Civil Code section 52.7
Student Online Personal Information Protection Act (SOPIPA) - California Business & Professions Code sections 22584 et seq.

Key takeaway: laws do not apply solely to location information but location information may fall within the defined protected information...
CALIFORNIA LAW

CCPA – California Consumer Privacy Act (effective July 1, 2020)

“personal information” = any information that “identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.”

Variety of new data elements that constitute PI including but not limited to: (1) identifiers such as any unique personal identifier or IP address; (2) electronic network activity information, including, browser histories, search history, and any information regarding a consumer’s interaction with a Web site, application or advertisement; (3) audio, electronic, visual, thermal, and olfactory information; and (4) geolocation data.

Any “inferences drawn” from various data elements of PI “to create a profile about a consumer reflecting the consumer’s preference, characteristics, psychological trends, preferences, predispositions, behavior, attitudes, intelligence, abilities and aptitudes” constitutes PI.

Consumer rights to (1) opt-out of sales and (2) deletion

Key takeaway: geolocation information is PI
## INDUSTRY SELF-REGULATION AND GUIDANCE

<table>
<thead>
<tr>
<th>Key principles:</th>
<th>Digital Advertising Alliance (DAA) self-regulatory framework</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disclosure and transparency</td>
<td>Network Advertising Initiative (NAI) self-regulatory framework</td>
</tr>
<tr>
<td>Consent and choice</td>
<td>Future of Privacy Forum Mobile Location Analytics Code of Conduct</td>
</tr>
<tr>
<td>Collection, retention, and use limitation</td>
<td>CTIA Best Practices and Guidelines for Location Based Services (wireless industry)</td>
</tr>
<tr>
<td>Security</td>
<td></td>
</tr>
<tr>
<td>Onward transfers</td>
<td></td>
</tr>
</tbody>
</table>

*privacy counsel™*
LOCATION TRACKING - ISSUES AND ETHICS

*Liberty* – free mobility without surveillance

*Privacy* – freedom from access to/misuse of intimate data, from intrusion, scrutiny by wrongdoers

*Ownership/monetization* – data subject versus collector

*Safety and security* – public interest, crime, terrorism

Who owns the data? Should there be substantive limits on collection and use or is disclosure and consent sufficient? Can effective consent be obtained?
LOCATION TRACKING - CONSENT

• FTC UDAP - not deceptive, “meaningful”
• CFPB UDAAP – not clear
• State UDAP – not clear
• CCPA opt-out of data selling (sharing)

• App developers/aggregators – consent to location tracking
• Sale of aggregated location data – no consent necessary?
LOCATION TRACKING – CONSENT

“Location History” = adding visual/locational movements to individual account Timeline automatically without real-time check-ins

“Web & App Activity” = collection of time-stamped GPS data through Google maps, searches, weather, and any other app and browser location data items

User must manually turn both off. Note: only impacts tracking by Google.

Google terms:

When Location History is off

• New location information is no longer saved to your Location History.
• Previous activity is not deleted from your Location History. You can manually delete your Location History.
• Your settings for other location services on your device, like Google Location Services and Find My Device, are not changed.
• Some location data may continue to be saved in other settings, like Web & App Activity, as part of your use of other services, like Search and Maps, even after you turn off Location History.
LOCATION TRACKING - CONSENT

GDPR – ICO Consent Checklist

☐ We have checked that consent is the most appropriate lawful basis for processing.
☐ We have made the request for consent prominent and separate from our terms and conditions.
☐ We ask people to positively opt in.
☐ We don’t use pre-ticked boxes or any other type of default consent.
☐ We use clear, plain language that is easy to understand.
☐ We specify why we want the data and what we’re going to do with it.
☐ We give separate distinct ('granular') options to consent separately to different purposes and types of processing.
☐ We name our organisation and any third party controllers who will be relying on the consent.
☐ We tell individuals they can withdraw their consent.
☐ We ensure that individuals can refuse to consent without detriment.
☐ We avoid making consent a precondition of a service.
☐ If we offer online services directly to children, we only seek consent if we have age-verification measures (and parental-consent measures for younger children) in place.

Key takeaways
- separate
- clear, plain, understandable language
- purpose specification
- granularity

Corollary
- use limitation
LOCATION TRACKING - CONSENT

GDPR

-thousands of data subject rights asserted post 5/25/18

-many included consent revocation

-most litigation re consent

-the predicate act problem
PRACTICE POINTERS

• Data inventory and access vectors
• Understanding of tech and capabilities
• Education and culture
• Privacy-by-design
• Disclosure/consent/opt-in or out
• Vendor management
• Impact assessments
PRACTICE RESOURCES

• Future of Privacy Forum  https://fpf.org

• International Association of Privacy Professionals https://iapp.org

• News media (WSJ, NYT, Google – “location tracking news”)
WHAT’S NEXT?
QUESTIONS?

pboshell@privacycounselllc.com

https://twitter.com/PrivacyCoLLC

https://www.linkedin.com/in/paige-boshell-76209910/

https://privacycounselllc.com

Please note that these materials and marks are copyrighted and owned by Privacy Counsel LLC. Content reproduced from third parties is the property of such parties and is reproduced here for educational purposes.