International Association of Privacy Professionals
Minneapolis/St. Paul KnowledgeNet: Mobile and Social Media Privacy

June 28, 2018

Melissa Krasnow
VLP Law Group LLP
Attorney biography:
https://www.vlplawgroup.com/attorneys/melissa-krasnow/

With thanks to Angela Scharf, University of Minnesota, for her help

Recent news

POLITICS

The New York Times

In Ruling on Cellphone Location Data, Supreme Court Makes Statement on Digital Privacy

By Adam Liptak

June 22, 2018

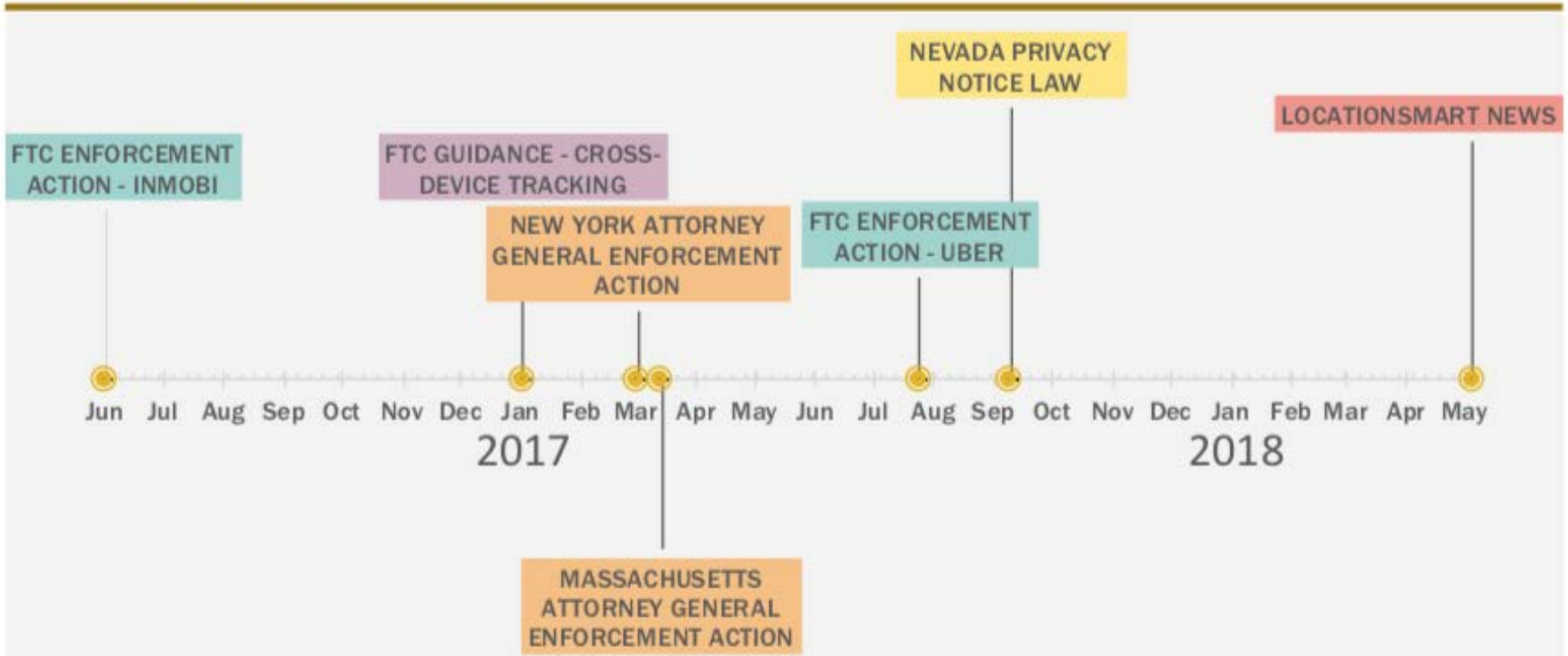
WASHINGTON — In a major statement on privacy in the digital age, the Supreme Court ruled on Friday that the government generally needs a warrant to collect troves of location data about the customers of cellphone companies.

"We decline to grant the state unrestricted access to a wireless carrier's database of physical location information," Chief Justice John G. Roberts Jr. wrote for the majority.

The 5-to-4 ruling will protect "deeply revealing" records associated with 400 million

The Supreme Court's ruling made a major statement on privacy in the digital age.
Tom Brenner/The New York Times

GEOLOCATION TIMELINE



DATE	Event
22-Jun	FTC enforcement action - InMobi
23-Jan	FTC guidance - cross-device tracking
23-Mar	New York attorney general enforcement action
4-Apr	Massachusetts attorney general enforcement action
15-Aug	FTC enforcement action - Uber
1-Oct	Nevada privacy notice law
26-May	LocationSmart news

FTC enforcement action

State enforcement action

State law

FTC guidance

Geolocation news

2018 geolocation news

This month, it emerged that the major mobile providers have been giving commercial third-parties the ability to instantly look up the precise location of any mobile subscriber in real time.

KrebsOnSecurity broke the news that one of these third parties — **LocationSmart** — leaked this ability for years to anyone via a buggy component on its Web site.

17 Tracking Firm LocationSmart Leaked Location Data for Customers of All Major U.S. Mobile Carriers Without Consent in Real Time Via Its Web Site

MAY 18

LocationSmart, a U.S. based company that acts as an aggregator of real-time data about the precise location of mobile phone devices, has been leaking this information to anyone via a buggy component of its Web site — *without the need for any password or other form of authentication or authorization* — KrebsOnSecurity has learned. The company took the vulnerable service offline early this afternoon after being contacted by KrebsOnSecurity, which verified that it could be used to reveal the location of any **AT&T**, **Sprint**, **T-Mobile** or **Verizon** phone in the United States to an accuracy of within a few hundred yards.

2018 geolocation news (con't)

We also learned that another California company — **Securus Technologies** — was selling real-time location lookups to a number of state and local law enforcement agencies, and that accounts for dozens of those law enforcement officers were obtained by hackers. Securus, it turned out, was ultimately getting its data from LocationSmart.

Source: https://krebsonsecurity.com/ (May 26, 2018)

Service Meant to Monitor Inmates' Calls Could Track You, Too

Cory Hutcheson, a former Missouri sheriff, was charged with using a private service to track people's cellphones without court orders. Mississippi County Sheriff Office

By Jennifer Valentino-DeVries

May 10, 2018

FTC reports: geolocation information as sensitive information

https://www.ftc.gov/reports/cross-device-tracking-federal-trade-commission-staff-report-january-2017

https://www.ftc.gov/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission

https://www.ftc.gov/news-events/press-releases/2012/03/ftc-issues-final-commission-report-protecting-consumer-privacy

2017 FTC enforcement action - Uber

….Uber stored sensitive consumer information, including geolocation information, in plain readable text in database back-ups stored in the cloud.

Source: https://www.ftc.gov/news-events/press-releases/2017/08/uber-settles-ftc-allegations-it-made-deceptive-privacy-data

FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

Contact | Stay Connect

ABOUT THE FTC | NEWS & EVENTS | ENFORCEMENT | POLICY | TIPS & ADVICE

Home » News & Events » Press Releases » Uber Settles FTC Allegations that It Made Deceptive Privacy and Data Security Claims

Uber Settles FTC Allegations that It Made Deceptive Privacy and Data Security Claims

Company failed to monitor access to, and provide reasonable security for, consumer data

SHARE THIS PAGE

FOR RELEASE

August 15, 2017

TAGS: Automobiles | Technology | Bureau of Consumer Protection | Consumer Protection | Privacy and Security | Consumer Privacy | Data Security

Note: *A conference call for media with FTC Acting Chairman Maureen K. Ohlhausen and Consumer Protection Acting Director Tom Pahl was held on August 15, 2017. FTC staff took questions from the media.*

Uber Technologies, Inc. has agreed to implement a comprehensive privacy program and obtain regular, independent audits to settle Federal Trade Commission charges that the ride-sharing company deceived consumers by failing to monitor employee access to consumer personal information and by failing to reasonably secure sensitive consumer

2017 FTC enforcement action – Uber (con't)

See also: https://www.vlplawgroup.com/blog/vlp-partner-melissa-krasnow-quoted-wall-street-journal-article-companies-can-learn-ubers-privacy-mistakes/

See also: https://www.vlplawgroup.com/blog/vlp-partner-melissa-krasnow-quoted-bloomberg-bna-article-uber-settles-ftc-customer-data-security-privacy-enforcement-action/

2016 FTC enforcement action - InMobi

Singapore-based mobile advertising company InMobi will pay $950,000 in civil penalties and implement a comprehensive privacy program to settle Federal Trade Commission charges it deceptively tracked the locations of hundreds of millions of consumers – including children – without their knowledge or consent to serve them geo-targeted advertising.

The FTC alleges that InMobi mispresented that its advertising software would only track consumers' locations when they opted in and in a manner consistent with their device's privacy settings. According to the complaint, InMobi was actually tracking consumers' locations whether or not the apps using InMobi's software asked for consumers' permission to do so, and even when consumers had denied permission to access their location information.

Source: https://www.ftc.gov/news-events/press-releases/2016/06/mobile-advertising-network-inmobi-settles-ftc-charges-it-tracked

2016 FTC enforcement action – InMobi (con't)

In addition, the company will be required to delete all information it collected from children, and will be prohibited from further violations of COPPA.

In addition, InMobi will be prohibited from collecting consumers' location information without their affirmative express consent for it to be collected, and will be required to honor consumers' location privacy settings. The company will also be required to delete the location information of consumers it collected without their consent and will be prohibited from further misrepresenting its privacy practices. The settlement also will require InMobi to institute a comprehensive privacy program that will be independently audited every two years for the next 20 years.

Source: https://www.ftc.gov/news-events/press-releases/2016/06/mobile-advertisingnetwork-inmobi-settles-ftc-charges-it-tracked

2013 FTC enforcement action - Goldenshores

Consumers also were presented with a false choice when they downloaded the app, according to the complaint. Upon first opening the app, they were shown the company's End User License Agreement, which included information on data collection. At the bottom of the license agreement, consumers could click to "Accept" or "Refuse" the terms of the agreement. Even before a consumer had a chance to accept those terms, though, the application was already collecting and sending information to third parties – including location and the unique device identifier.

Source: https://www.ftc.gov/news-events/press-releases/2013/12/android-flashlight-app-developer-settles-ftc-charges-it-deceived

2013 FTC enforcement action - Goldenshores (con't)

The settlement with the FTC prohibits the defendants from misrepresenting how consumers' information is collected and shared and how much control consumers have over the way their information is used. The settlement also requires the defendants to provide a just-in-time disclosure that fully informs consumers when, how, and why their geolocation information is being collected, used and shared, and requires defendants to obtain consumers' affirmative express consent before doing so.

The defendants also will be required to delete any personal information collected from consumers through the Brightest Flashlight app.

Source: https://www.ftc.gov/news-events/press-releases/2013/12/android-flashlight-app-developer-settles-ftc-charges-it-deceived

State privacy policy laws and the GDPR: geolocation information as personally identifiable information

California Online Privacy Protection Act

Delaware Online Privacy and Protection Act

Nevada privacy notice law

See: https://www.irmi.com/articles/expert-commentary/nevada-passes-new-privacy-notice-law and see also: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375

GDPR: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en#examples-of-personal-data

2017 Massachusetts attorney general enforcement action

In its advertising campaign, Copley set mobile geofences at or near reproductive health centers and methadone clinics in Columbus, New York City, Pittsburgh, Richmond, and St. Louis. When a consumer entered the geofenced area near these locations, Copley tagged the consumer's device ID and served advertisements to the consumer's device for up to 30 days.

Source: http://www.mass.gov/ago/news-and-updates/press-releases/2017/2017-04-04-copley-advertising-geofencing.html

2017 Massachusetts attorney general enforcement action (con't)

The settlement, resolved through an Assurance of Discontinuance filed today in Suffolk Superior Court, resolves allegations that Copley's practices would violate consumer protection laws in Massachusetts by tracking a consumer's physical location near or within medical facilities, disclosing that location to third-party advertisers, and targeting the consumer with potentially unwanted advertising based on inferences about his or her private, sensitive, and intimate medical or physical condition, all without the consumer's knowing consent.

The settlement assures that Copley will not use geofencing technology at or near Massachusetts healthcare facilities to infer the health status, medical condition, or medical treatment of any individual.

Source: http://www.mass.gov/ago/news-and-updates/press-releases/2017/2017-04-04-copley-advertising-geofencing.html

2017 New York attorney general enforcement action

The Attorney General's investigation revealed that two app developers claimed that their apps accurately measured heart rate after vigorous exercise using only a smartphone camera and sensors. A third developer claimed that its app transformed a smartphone into a fetal heart monitor and therefore could be used to play an unborn baby's heart rate, even though the app was not an FDA-approved fetal heart monitor. The three developers initially marketed these apps without possessing sufficient information to back up their marketing claims, but have since cooperated with the Office of the Attorney General to revise their advertising, consumer warnings and privacy practices.

Source: https://ag.ny.gov/press-release/ag-schneiderman-announces-settlements-three-mobile-health-application-developers

2017 New York attorney general enforcement action (con't)

Under the Attorney General's settlements, the developers agreed to provide additional information about testing of the apps, to change their ads to make them non-misleading, and to pay $30K in combined penalties to the Office of the Attorney General. Additionally, the developers now post clear and prominent disclaimers informing consumers that the apps are not medical devices and are not approved by the FDA.

The developers also made changes to protect consumers' privacy. The developers now require affirmative consent to their privacy policies for these apps and disclose that they collect and share information that may be personally identifying. This includes users' GPS location, unique device identifier, and "deidentified" data that third parties may be able to use to reidentify specific users.

Source: https://ag.ny.gov/press-release/ag-schneiderman-announces-settlements-three-mobile-health-application-developers