2019

Data Generated by New Technologies and the Law: A Guide for Massachusetts Practitioners

Andrew Sellars

Data Generated by New Technologies and The Law, 2019 Edition

This handout is presented as part of the *When New Technologies Become Evidence* presentation provided by MCLE New England, and focuses on the different forms of consumer technologies that are becoming popular and how data generated by these technologies is being used for law enforcement, especially as part of pre-trial investigations. Notable state and federal cases from Massachusetts are noted throughout.

I. Getting data from a service provider – a quick overview of the Stored Communications Act

Modern digital devices are part machine and part service. Digital devices usually have accompanying service providers that send and receive data from a device, and in turn have access to data about the device and its owner. When law enforcement begins investigations, it will often start on the service-provider side, as one can obtain data from these services without alerting the investigation target.

The Stored Communications Act (18 U.S.C. § 2701 et seq.) sets the rules for accessing various forms of information stored by an "electronic communications service" or a "remote computing service" – which generally includes many modern online platforms and services. This handout begins with a quick reference table for this law, before exploring its application to different types of technologies.

The law has a peculiar structure and a fair number of caveats and exceptions, but generally speaking one can break the law down by first examining the type of record law enforcement seeks to access, and then inquiring whether the service provider in question is offered to the public or not. From there, this table reviews whether the service provider can voluntarily disclose the information or whether it must be compelled — and if so, what legal process must the compulsory disclosure follow:[1]

Type of Record	**Services Offered to the Public**		**Non-Public Services**	
	Can the service voluntarily disclose the information?	**What level of process is required for the government to compel disclosure?**	**Can the service voluntarily disclose the information?**	**What level of process is required for the government to compel disclosure?**
Contents of user communications (emails, messaging applications, etc.)	No, absent a specific exception in § 2702(b) (e.g., to the intended recipient, with user consent, etc.).	Major platforms all require a *search warrant*. By statute, unopened messages that are stored for less than 180 days require a *search warrant*, and all others can be obtained by *search warrant* or at *2703(d) order*. The Sixth Circuit in *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010) found this part of the SCA to violate the Fourth Amendment, and now most platforms wait for a *search warrant*.	The SCA does not prevent it.	Same as with public service providers, but as non-public providers are often at liberty to voluntarily disclose such records they may opt to comply with a lower standard.

[1] This table is based on a similar table in Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1223 (2004).

Type of Record	Services Offered to the Public		Non-Public Services	
	Can the service voluntarily disclose the information?	**What level of process is required for the government to compel disclosure?**	**Can the service voluntarily disclose the information?**	**What level of process is required for the government to compel disclosure?**
Contents in a "remote computing service"	No, absent a specific exception in § 2702(b).	Major platforms require a *search warrant*. By statute, can be obtained through a *search warrant* without notice to user or can be obtained with notice (although notice can often be delayed under § 2705) by *2703(d) order* or *subpoena*. After *Warshak*, 631 F.3d 266, found the section concerning emails unconstitutional, platforms generally require a *search warrant*.	The SCA does not prevent it.	The SCA does not apply – "remote computing services" under the SCA are defined as solely those offered to the public under § 2711(2).
Most non-content records	To a non-gov't entity, the SCA does not prevent it. To the gov't, no, absent an exception in § 2702(c).	Can be compelled through a *search warrant*, or *2703(d) order.* Some special rules in investigations of telemarketing fraud. No notice to user required.	The SCA does not prevent it.	Same as with public service providers, but as non-public providers are often at liberty to voluntarily disclose such records they may opt to comply with a lower standard.
Basic subscriber information (name, address, credit card, system logs, IP addresses, etc.)	To a non-gov't entity, the SCA does not prevent it. To the gov't, no, absent an exception in § 2702(c).	Can be compelled through a *search warrant*, a *2703(d) order*, or a *subpoena*. No notice to user required.	The SCA does not prevent it.	Same as with public service providers, but as non-public providers are often at liberty to voluntarily disclose such records they may opt to comply with a lower standard.

The 2703(d) order is an intermediate standard of compulsory disclosure more substantial than a subpoena but less burdensome than a warrant, created specifically for the Stored Communications Act. Under it, the government must show "specific and articulable facts showing that there are reasonable grounds to believe that the [contents and information] are relevant and material to an ongoing investigation."[2]

II. New Technologies and Types of Information

The following sections break down some common types of emerging technologies, the forms of data that they generate, and who likely has access to that data. Each section also includes some noteworthy cases and emerging topics of discussion.

[2] 18 U.S.C. § 2703(d).

A. Cell Phones / Smartphones

Pew Research Center now estimates that 96% of the U.S. population owns a cell phone of some kind, and 81% own a smartphone, up from 83% and 35%, respectively, in 2011.[3] *Examples*: Apple iPhone, Samsung Galaxy, Google Pixel, LG Stylo.

Data Collected:

- *Location*: "Cell Site Location Information" (CSLI) can be calculated by an onboard GPS chip, triangulating distance from phones and nearby towers, and in some cases, triangulation through nearby Wi-Fi connections. Collecting CSLI is now the subject of extensive analysis under the Fourth Amendment and Article 14 of the Massachusetts Declaration of Rights.[4] Data could be stored on the device, with the cell service carrier, or in the case of Wi-Fi access, on the logs of the Wi-Fi service devices or those providing WiFi connections. Service providers frequently also make this data available to others, though there has been increased scrutiny and litigation aimed to mitigate that practice.[5]
- *Contents of voice calls*: transmitted live, but not often stored by any party due to strict limitations under state and federal wiretapping laws. Both private and government interception is regulated. Government interception is subject to "super-warrant" standard, including demonstrations of exhaustion and the suspected commission of certain serious crimes.
- *Metadata around voice calls*: transmitted live and often recorded and stored by cell carriers for billing and other purposes. Some data may also be stored on the device. Live interceptions are subject to the pen register statute, 18 U.S.C. § 3121 *et seq*. Stored metadata records are subject to the Stored Communications Act.
- *Photographs and other user-recorded content*: virtually all modern phones have a camera and store photos taken on the phone. Images may be stored and retrieved locally or synchronized with a cloud-based data service (e.g., Apple iCloud, Google Photos), and retrieved from such platform. They may also be backed up to a home computer or other device.
- *Sensory instrumentation data from applications*: a user may have installed applications which store various forms of data from a phone, including data derived from a phone's accelerometer and related sensors (including gyroscopes and magnometers), which tracks the phone's orientation and movement, and can be used to infer movement pace and steps taken. More sophisticated smartphones include ambient light sensors, barometers, and other forms of sensory instrumentation. Some of this material may be stored and retrieved through the phone's operating system. Other data may be stored on specific applications that track such sensors, such as fitness apps, which may be retrieved locally or obtained from the app's online platform.[6]

---

[3] *Mobile Fact Sheet*, PEW RESEARCH CTR., http://www.pewinternet.org/fact-sheet/mobile/ (last updated June 12, 2019).

[4] *See, e.g.*, Carpenter v. United States, 138 S. Ct. 2206 (2018); Commonwealth v. Augustine, 467 Mass. 230 (2014).

[5] *See* Joseph Cox, *I Gave a Bounty Hunter $300. Then He Located Our Phone*, MOTHERBOARD (Jan. 8, 2019), https://www.vice.com/en_us/article/nepxbz/i-gave-a-bounty-hunter-300-dollars-located-phone-microbilt-zumigo-tmobile; *EFF Sues AT&T, Data Aggregators for Giving Bounty Hunters and Other Third Parties Access to Customers' Real-Time Locations*, ELEC. FRONTIER FOUND. (July 16, 2019), https://www.eff.org/press/releases/eff-sues-att-data-aggregators-giving-bounty-hunters-and-other-third-parties-access.

[6] For more detail, see David Nield, *All the Sensors in Your Smartphone, And How They Work*, GIZMODO (July 23, 2017), https://fieldguide.gizmodo.com/all-the-sensors-in-your-smartphone-and-how-they-work-1797121002.

Notes and Cases:

- Search of contents of phone incident to arrest now subject to higher Fourth Amendment standards after *Riley v. California*.[7] The Supreme Judicial Court has extended the logic of *Riley* to digital cameras.[8]
- In addition to the collection of CSLI described above, cell carriers have the ability to directly query, or "ping" a subscriber's present location. The Supreme Judicial Court recently ruled that such a ping is a search under the Massachusetts Declaration of Rights.[9]
- Smartphones are often protected by passwords, and compelling users to reveal their passwords may raise Fifth Amendment concerns. The Supreme Judicial Court recently found that law enforcement could compel entry of a password if it can show beyond a reasonable doubt that the suspect knows the password.[10] Compelled unlocking of phones using biometric identifiers, such facial recognition or fingerprint scans, is not typically seen to raise a Fifth Amendment concern, with some notable contrary cases.[11]
- Despite increased constitutional sensitivity regarding location information, the phone carriers still sell customer location information to private companies, some of whom in turn sell customer location information to government and non-government parties. This does not violate the text of the Stored Communications Act, but it is unclear after *Carpenter* and *Augustine* whether this raises an issue under the Fourth Amendment.[12] There are numerous private lawsuits also aimed at curtailing the practice.[13]
- A case pending in the District of Massachusetts will determine whether the logic of cases like *Riley* also means that customs agents may no longer rely on the Fourth Amendment's border search exception to search electronic devices. The court heard oral argument in the case on July 18, 2019.[14]

---

[7] 134 S. Ct. 2473 (2014); *see also* United States v. Wurie, 728 F.3d 1 (1st Cir. 2013), *aff'd sub nom. Riley*, 134 S. Ct. 2473.

[8] Commonwealth v. Mauricio, 477 Mass. 588 (2017) (applying Art. 14 Mass. Decl. Rights).

[9] Commonwealth v. Almonor, 482 Mass. 35 (2019). For a contrary approach under the Fourth Amendment, see United States v. Riley, 858 F.3d 1012 (6th Cir. 2017).

[10] Commonwealth v. Jones, 481 Mass. 540 (2019); *see also* Commonwealth v. Gelfgatt, 468 Mass. 512 (2014); In re Grand Jury Investigation, 92 Mass. App. Ct. 531 (2017); United States v. Apple MacPro Computer, 851 F.3d 238 (3d Cir. 2017); In re Grand Jury Subpoena, 670 F.3d 1335 (11th Cir. 2012). The SJC noted in *Jones* that "the analysis would be different had the Commonwealth sought to compel the defendant to produce specific files located in the contents of the . . . phone." *Jones*, 481 Mass. at 548 n.10.

[11] *See* Commonwealth v. Baust, No. CR14-1439, 2014 WL 10355635 (Va. Circuit Ct. 2014); State v. Diamond, 890 N.W.2d 143 (Minn. Ct. Appeals 2017); *but see* In re Application for Search Warrant, 236 F. Supp. 3d 1066 (N.D. Ill. 2017) (rejecting a warrant application requesting fingerprint to unlock phone, citing Riley v. California, 134 S. Ct. 2473 (2014)); In re Residence in Oakland, Cal., 354 F. Supp. 3d 1010 (N.D. Cal. 2019) (rejecting warrant requiring all persons found at location of search to surrender biometric features as overbroad).

[12] *See* Zach Whittaker, *US Cell Carriers Are Selling Access to Your Real-Time Phone Location Data*, ZDNET (May 14, 2018), https://www.zdnet.com/google-amp/article/us-cell-carriers-selling-access-to-real-time-location-data/. A recent class action complaint alleges that AT&T's sharing of this data violates the Federal Communications Act, 47 U.S.C. § 222. *See* Complaint, Scott v. AT&T, No. 19-cv-4063 (N.D. Cal. filed July 16, 2019), *available at* https://www.eff.org/document/scott-v-att-geolocation-complaint.

[13] *See supra* note 4; Jon Brodkin, *Verizon and AT&T Will Stop Selling Your Phone's Location to Data Brokers*, ARS TECHNICA (June 19, 2018), https://arstechnica.com/tech-policy/2018/06/verizon-and-att-will-stop-selling-your-phones-location-to-data-brokers/. Some litigants are also bringing privacy tort challenges against those who track their location using GPS and similar technologies. *See, e.g.*, Demo v. Kirksey, No. 18-cv-716, 2018 WL 5994995 (D. Md. Nov. 15, 2018).

[14] *See* Alassad v. Nielsen, No. 17-cv-11730, 2018 WL 2170323 (D. Mass. May 9, 2018).

B. Facial Analysis Technology

A growing number of advocates and policymakers have raised alarm over the increased use and deployment of facial analysis technology for both government and private purposes.[15] The technology has been in public use for nearly two decades,[16] but has risen to the fore in light of the rapid commercialization of artificial intelligence, and with it, growing public attention and discussion of its use and impact.[17]

Unlike the various consumer devices categorized in this handout, facial analysis technology is a form of computation that is used across many forms of devices. Indeed, nearly every other category of device in this handout has the potential to use facial analysis in some way, be that as a biometric identifier to unlock a smartphone, on social media platforms to detect friends' faces in uploaded photos and videos, or in "Internet of Things" devices like smart doorbells to differentiate between house occupants and others.

Data Collected:

- *Facial geometry*: most facial recognition technologies operate by taking a photo or video of a person's face and using a "trained" algorithm to detect features on the face. One can then take measurements of the relative distance and angle between the the different features on the face to develop a facial geometry profile (sometimes called a "faceprint"), which is then matched against a database to identify a face.[18] Depending on how the technology is deployed, the company will save some combination of the faceprint, the reference database of faceprints, original photos and videos, and other metadata around the performance of the technology. Courts have yet to analyze how such records may be retrieved under the Stored Communications Act. Three states now have "biometric privacy" statutes that limit some collection and use of faceprints, but none appear to place meaningful restrictions on how law enforcement may obtain such data.[19]
- *"Trained" algorithms and their training data*: the detection of elements of a face from a photograph or video is usually done by a machine learning algorithm operating on the service provider's computers,

---

[15] *See, e.g.*, Luke Stark, *Facial Recognition is the Plutonium of AI*, 25 XRDS 50 (2019), *available at* https://starkcontrast.co/s/Facial-Recognition-is-Plutonium-Stark.pdf.

[16] One of the first documented uses in public was at the Super Bowl in 2001. Kaleigh Rogers, *That Time the Super Bowl Secretly Used Facial Recognition Software on Fans*, MOTHERBOARD (Feb. 7, 2016), https://www.vice.com/en_us/article/kb78de/that-time-the-super-bowl-secretly-used-facial-recognition-software-on-fans.

[17] For an extensive review of contemporary concerns with facial analysis technology and other forms of artificial intelligence, see Meredith Whittaker et al., *AI Now Report 2018*, AI NOW INSTITUTE (Dec. 2018), https://ainowinstitute.org/AI_Now_2018_Report.pdf.

[18] *See Face Recognition*, ELEC. PRIVACY INFO. CTR., https://www.epic.org/privacy/facerecognition/ (last visited July 22, 2019).

[19] *See* 740 ILCS 14/15(d)(3), (4) (Illinois); Tex. Bus. & Com. §§ 503.001(c)(1)(C), (D) (Texas); Wash. Rev. Code § 19.375.020(3)(f) (Washington State). Of the three, Texas is the only state that requires disclosure to law enforcement be made "in response to a warrant," Tex. Bus. & Com. § 503.001(c)(1)(D), but it also allows for disclosure as "required or permitted by federal statute," § 503.001(c)(1)(C), which could be interpreted to cover compelled disclosure under the Stored Communications Act. The Massachusetts legislature is presently considering a bill which would introduce similar biometric privacy obligations, though it too would not place greater burdens on law enforcement requests for faceprints. *See* S.120 § 8(a)(2), 191st Leg. (Mass. 2019).

which is "trained" through exposure to numerous other, categorized data.[20] Companies typically safeguard such "trained" algorithms as trade secrets and zealously guard against their disclosure, presenting obvious concerns for transparency and accountability. Such algorithms would not be subject to disclosure under the Stored Communications Act, and courts have resisted compelling disclosure of other types of "trained" machine learning algorithms as part of criminal proceedings out of trade secret concerns.[21] Sets of training data are similarly kept secret by companies.

- *Predictions drawn from algorithms:* the outputs of machine learning algorithms are usually either disclosed overtly as part of their use, or used as part of the technology's operation (e.g., to unlock the phone, label the face in social media, or alert the homeowner of an unrecognized person at the door). While the prediction is usually explicitly available, the calculation behind the prediction often is not.

Notes and Cases:

- Facial analysis technology is one of only a few technologies for which multiple experts have called for a total or near-total prohibition on its adoption, at least in the short term.[22] In June 2019 the City of Somerville passed an ordinance completely prohibiting the use of "face surveillance systems" by the city or city officials.[23] Similar bans now exist in San Francisco and Oakland,[24] and the City of Cambridge is presently contemplating a similar move.[25]
- Use of facial analysis technology has catalyzed other forms of government data sharing. A recent investigation by Georgetown's Center on Privacy and Technology revealed that FBI and ICE agents have made thousands of requests to access drivers' license photographs stored in state motor vehicle

---

[20] "Machine learning" algorithms generally have a "classifier" function that will make a prediction of an output based on recognizable inputs (for example, predicting that an area of an image is a nose on a face, based on surrounding colors, shapes, and lines), and a "learning" function that will fine-tune the classifier by processing data that is already labelled with the correct output, and using it to adjust the weights given to different variables in the classifier (for example, using images with labeled noses to adjust how much weight the classifier places on different colors, shapes, and lines in future images). *See* Jenna Burrell, *How the Machine "Thinks": Understanding Opacity in Machine Learning Algorithms*, 3 BIG DATA & SOCIETY 1 (2016), *available at* https://journals.sagepub.com/doi/pdf/10.1177/2053951715622512.

[21] For an extensive review of how trade secrets and other intellectual property claims can hinder access to algorithms in criminal cases, see Rebecca Wexler, *Life, Liberty, and Trade Secrets*, 70 STAN. L. REV. 1343 (2018), *available at* https://www.stanfordlawreview.org/print/article/life-liberty-and-trade-secrets/.

[22] *See* Stark, *supra* note 15; *ACLU Comment on Microsoft Call for Federal Action on Face Recognition Technology*, ACLU (July 13, 2018), https://www.aclu.org/press-releases/aclu-comment-microsoft-call-federal-action-face-recognition-technology ("Congress should take immediate action to put the brakes on this technology with a moratorium on its use by government, given that it has not been fully debated and its use has never been explicitly authorized."); Woodrow Hartzog & Evan Selinger, *Facial Recognition Is the Perfect Tool for Oppression*, MEDIUM (Aug. 2, 2018), https://medium.com/s/story/facial-recognition-is-the-perfect-tool-for-oppression-bc2a08f0fe66 ("[W]hen technologies become so dangerous, and the harm-to-benefit ratio becomes so imbalanced, categorical bans are worth considering.").

[23] City of Somerville Ordinance 2019-16 (June 27, 2019), *available at* https://library.municode.com/ma/somerville/ordinances/code_of_ordinances?nodeId=966223.

[24] Caroline Haskins, *Oakland Becomes Third U.S. City of Ban Facial Recognition*, MOTHERBOARD (July 17, 2019), https://www.vice.com/en_us/article/zmpaex/oakland-becomes-third-us-city-to-ban-facial-recognition-xz.

[25] Kade Crockford, *Cambridge to Take Up Face Surveillance Ban*, PRIVACY SOS (July 26, 2019), https://privacysos.org/blog/cambridge-to-take-up-face-surveillance-ban/. The City of Boston appears to be moving in a different direction on the matter. The city was caught a few years ago testing facial analysis technology on the attendees of the "Boston Calling" music festival without their knowledge or consent, and has not ruled out future use of the technology. *See* Chris Faraone et al., *Boston Trolling (Part 1): You Partied Hard at Boston Calling and There's Facial Recognition Data to Prove It*, DIGBOSTON (August 7, 2014), https://digboston.com/boston-trolling-part-i-you-partied-hard-at-boston-calling-and-theres-facial-recognition-data-to-prove-it/.

departments.[26] The ACLU of Massachusetts has filed a lawsuit seeking records from the Massachusetts Department of Transportation about MassDOT's sharing of license photographs for facial surveillance and analysis.[27]

- Multiple studies have now demonstrated that facial recognition algorithms have greater rates of error among darker-skinned and female faces.[28] While the criminal justice system has developed some techniques for addressing eyewitness misidentification by persons of another race or ethnic group,[29] no similar evidentiary doctrines have been developed to address the bias in machine systems.
- No court appears to have analyzed whether use of facial recognition technology in the public should constitute a search under the Fourth Amendment.[30]

C. Social Media Platforms

Websites and mobile applications where users can create accounts, log in, and share content with one another. About 72% of adults in the United States use some form of social media platform, up from about 50% in 2011.[31] *Examples:* Facebook, Twitter, Instagram, Snapchat.

Data Collected:

- *User-submitted content*: users routinely and voluntarily upload photos, videos, and text. Such information is typically made public, and therefore can be retrieved without any legal process. Occasionally, metadata embedded within photographs can provide even further information, including the location where the photo is taken and the type of camera used, although many platforms remove such metadata as part of the image uploading process. Data stored on platform and likely retrievable by both the platform and the user.
- *Peer-to-peer messages*: many platforms allow users to send messages to each other within the platform. Many platforms store those messages in a way that the service can observe them, and thus could respond to process to produce them. The user also likely has access to this information.

---

[26] Drew Harwell, *FBI, ICE Find State Driver's License Photos are a Gold Mine for Facial-Recognition Searches*, WASH. POST. (July 7, 2019), https://www.washingtonpost.com/technology/2019/07/07/fbi-ice-find-state-drivers-license-photos-are-gold-mine-facial-recognition-searches/. The Driver's Privacy Protection Act places restrictions on the dissemination of driver's license photographs, but exempts sharing to government agencies. 18 U.S.C. § 2721(b)(1).

[27] ACLU of Mass. v. Mass. Dep't of Transportation, No. 1984CV02193D (Mass. Super. Suffolk filed July 10, 2019), *available at* https://www.aclum.org/sites/default/files/field_documents/20190710_aclu-massdot.pdf. MassDOT admits that it shares photographs on a case-by-case basis, but denies granting systematic access to state or federal law enforcement. Michael P. Norton, *ACLU Sues MassDOT For Details On Its Driver's License Database And Face Surveillance Uses*, WBUR (July 10, 2019), https://www.wbur.org/news/2019/07/10/aclu-massdot-facial-recognition-lawsuit.

[28] A pathbreaking study on the topic found the maximum error rate on gender detection for lighter-skinned male faces among four leading facial analysis companies at 0.8%, whereas darker-skinned female faces had error rates of up to 34.7%. Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, 81 PROCEEDINGS OF MACHINE LEARNING RESEARCH 1 (2018), *available at* http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf*; see also* Tom Simonite, *The Best Algorithms Struggle to Recognize Black Faces Equally*, WIRED (July 22, 2019), https://www.wired.com/story/best-algorithms-struggle-recognize-black-faces-equally/.

[29] *See, e.g.*, Commonwealth v. Bastaldo, 472 Mass. 16 (2015) (developing rules on jury instructions concerning cross-racial and cross-ethnic misidentification by eyewitnesses).

[30] CLARE GRAVE ET AL., THE PERPETUAL LINE-UP: UNREGULATED POLICE FACE RECOGNITION IN AMERICA, GEORGETOWN CTR. ON PRIVACY & TECH. at 35 (2016), available at https://www.perpetuallineup.org/report.

[31] *Social Media Fact Sheet*, PEW RESEARCH CTR., https://www.pewinternet.org/fact-sheet/social-media/ (last updated June 12, 2018).

- *HTTP header information*: as part of the standard way in which website hosts communicate with users through the Hypertext Transfer Protocol, platforms are exposed a variety of information about the user's web browser, including the user's IP address, browser type (e.g., Firefox, Chrome, Safari, etc.) and version number, the address of the site last visited by the user, and other web configuration information. Such information could be unique enough to develop a persistent profile of a user, even when the user is not logged in.[32] Many platforms preserve some or all of that information to track website analytics, though many only preserve it in an aggregate form. Users can provide a current version of this information from their present browser configuration, but unlikely to hold historical versions of that information.
- *On-site access logs:* many commercial websites use a variety of other tracking techniques to monitor user engagement with platforms, including cookies (which track a given user across different sections of a website), scripts that send additional information from a user's computer to a website, "fingerprinting" through creative use of configuration information that a browser makes available,[33] and "session replay scripts" that follow a user's actual keyboard and mouse inputs while they are on the platform.[34] Data is stored on platform. Some platforms — including Facebook[35] — make some of this information available to users upon request, but many do not.
- *Mobile device information*: when accessing a social media application from a smartphone, the application is exposed to some of the sensor, location, and other data described above. It may also collect information from your phone's contact lists, call history, and messaging history.[36] This data may be stored and disclosed by the platform.

Notes and Cases:

- Courts have looked to a user's privacy settings to determine whether they have shown a reasonable expectation of privacy in their social media content, and will deny claims when the user has displayed the relevant content publicly.[37]
- The content of publicly-displayed messages can sometimes reveal more than suspects would wish. Last year, investigators in the UK were able to identify a suspect after he posted a photo on WhatsApp showing him holding ecstasy tablets in the palm of his hand. Investigators were able to identify the suspect's fingerprints though examination of the photo.[38]

---

[32] *See Panopticlick: Is Your Browser Safe Against Tracking?*, ELEC. FRONTIER FOUND., https://panopticlick.eff.org/about (last visited July 29, 2019).

[33] Chris Smith, *Here are Over 5,000 Sites that Track You with Canvas Fingerprinting*, BGR (July 24, 2014), https://bgr.com/2014/07/24/canvas-fingerprinting-what-sites-use-it/.

[34] Steven Englehardt, *No Boundaries: Exfiltration of Personal Data by Session-Replay Scripts*, FREEDOM TO TINKER, https://freedom-to-tinker.com/2017/11/15/no-boundaries-exfiltration-of-personal-data-by-session-replay-scripts/ (Nov. 15, 2017).

[35] Louise Matsakis, *What To Look For In Your Facebook Data — And How To Find It*, WIRED (March 28, 2018), https://www.wired.com/story/download-facebook-data-how-to-read/.

[36] Tom Warren, *Facebook Has Been Collecting Call History and SMS Data from Android Devices*, THE VERGE (March 25, 2018), https://www.theverge.com/2018/3/25/17160944/facebook-call-history-sms-data-collection-android.

[37] *See* United States v. Westley, No. 17-cr-171, 2018 WL 3448161 (D. Conn. July 17, 2018); *see also* United States v. Mereglido (S.D.N.Y. 2012) ("Whether the Fourth Amendment precludes the Government from viewing a Facebook user's profile absent a showing of probable cause depends, *inter alia*, on the user's privacy settings."); United States v. Shipp, No. 19-cr-29, 2019 WL 3082484 (E.D.N.Y. July 15, 2019).

[38] Chris Wood, *WhatsApp Photo Drug Dealer Caught by "Groundbreaking" Work*, BBC NEWS (April 15, 2018), https://www.bbc.com/news/uk-wales-43711477.

- Image metadata can be an atypical way to obtain location information. Vice Magazine in 2012 accidentally revealed the secret location of John McAfee, who at the time was wanted by authorities in Belize, by uploading a photo of a journalist with McAfee. The file for the digital photo contained metadata that revealed the location where the photo was taken, and thus revealed McAfee's hideout in Guatemala.[39]

D. Secure Messaging Services

A number of companies now offer messaging services that promise to be more private and secure than standard SMS or social media messaging. Many do so through use of end-to-end encryption of messages between parties, though most commercial deployments of end-to-end encryption services also include other mechanisms for surveillance, depending on configuration. *Examples:* WhatsApp, Signal, Telegram, iMessage.

Data Collected:

- *(Encrypted) contents of messages/calls:* messaging services in this category tend to provide end-to-end encryption on messages, meaning that the platform is not put in the position of possessing the content of the message in an easily-readable form. For most cases this will mean that the platform will not provide any useful material, but more sophisticated cases or situations with poorly designed or deployed encryption systems may provide means to decrypt and reveal the contents of messages. In most systems both the sender and recipient will have access to these messages in an unencrypted form.
- *Metadata around calls:* even if the particular contents of messages are difficult for a platform to reveal, most forms of secure messaging collect various additional information about a user's availability, access to the platform, and the to/from information around messages. Some of these are essential and unavoidable when providing a communications service, and some are collected for convenience or performance improvements. The platform will have access to much of that information from routing messages, and can disclose or place real-time surveillance around such information pursuant to the proper legal process.
- *Account information:* like all online services, secure messaging services may have basic account information, billing information, and other information shared when signing up. Many of these platforms take steps to limit this information as much as possible, though what information they collect is retrievable from the platform.

Notes and Cases:

- Even if the system is set up in a way to "forget" or encrypt as much data about a user as possible, the operation of the service may necessarily expose a platform to content and metadata about customers, and law enforcement may be able to capture information at the moment such exposed information is in the platform's possession. For example, during the investigation into Edward Snowden's leaks of NSA information, federal investigators got a court to order for the secure email service Lavabit to track the IP addresses used to access the email account in real time, despite the company taking steps to avoid ever preserving such information.[40]
- End-to-end encryption of messages also doesn't mean that investigators cannot obtain messages through other means. Special Counsel Robert Muller's investigation into Paul Manafort used the contents of messages from an encrypted service to show that Manafort allegedly attempted to tamper with witnesses in his case. Two witnesses who received such messages voluntarily turned them over to law enforcement,

---

[39] Michael Zhang, *EXIF Data May Have Revealed Location of Fugitive Software Tycoon John McAfee*, PETAPIXEL (Dec. 3, 2012), https://petapixel.com/2012/12/03/exif-data-may-have-revealed-location-of-fugitive-billionaire-john-mcafee/.

[40] *See* In re Sealed Case, 749 F.3d 276 (4th Cir. 2014) (finding Lavabit failed to preserve its objection to the pen register order in that case).

and Manafort voluntarily backed up messages onto Apple's iCloud, thus exposing that information to Apple, who then turned it over to authorities in response to legal process.[41]

- The use of strong, end-to-end encrypted messaging services has long been a point of contention and opposition between civil liberties organizations and law enforcement (a debate that, along with encryption of devices themselves, has been nicknamed the "crypto wars"). Department of Justice leadership under multiple administrations have called for some form of workaround of encryption to afford access for law enforcement, most recently by Attorney General Barr in testimony before Congress in July 2019.[42] More sophisticated proposals allow for uncompromised encryption, but ask service providers to conduct client-side scanning for contraband materials, insert "ghost" law enforcement users into user-to-user communications upon request, or have end-to-end encryption off by default.[43]

E. Fitness Trackers and Smartwatches

A growing number of persons wear digital fitness trackers to monitor their own health and activity. These devices are sometimes independent and sometimes combined with "smartwatches" with embedded accelerometers. *Examples*: Apple Watch, FitBit Flex, Garmin Vivosport, TomTom Spark.

Data Collected:

- *Steps and other physical activity:* the defining characteristic of most fitness trackers is their calculation of steps, usually done through an onboard accelerometer that combines data about movement with band orientation and force of impact to discern footsteps from other motion. Such information is typically transmitted to the service provider's servers via a connection between a user's device and their smartphone, combined with an onboard application. Step data is usually available to a user through their smartphone app, and stored with the service provider.
- *Location:* some devices may also have an onboard GPS chip, which has the potential to track location at the same level of granularity as smartphones, discussed above. This data may be stored on the user's smartphone if logged through some application (such as a running app that tracks a runner's route), and may also be stored by the service provider.
- *Heart rate:* many fitness trackers use optical sensors pointed towards a user's wrist to measure blood flow through their capillaries, which is then used to calculate a heart rate. This is a rough estimation, and researchers have found that these devices can often misrepresent a user's heart rate when not accompanied

---

[41] *See* Lorenzo Franceschi-Bicchierari, *Paul Manafort's Terrible Encrypted Messaging OPSEC Got Him Additional Charges*, MOTEHRBOARD (June 5, 2018), https://motherboard.vice.com/en_us/article/zm8q43/paul-manafort-icloud-whatsapp-bad-opsec-witness-tampering.

[42] Patrick Howell O'Neill, *Barr's Call for Encryption Backdoors Has Reawakened a Years-Old Debate*, MIT TECH. REVIEW (July 24, 2019), https://www.technologyreview.com/s/614003/trumps-justice-department-calls-for-encryption-backdoor-law/; *see also* Jon Brodkin, *Trump's DOJ Tries to Rebrand Weakened Encryption as "Responsible Encryption"*, ARS TECHNICA (Oct. 10, 2017), https://arstechnica.com/tech-policy/2017/10/trumps-doj-tries-to-rebrand-weakened-encryption-as-responsible-encryption/. Technologists have routinely pointed out that such "compromises" on encryption universally degrade the quality of security. HAROLD ABELSON ET. AL, KEYS UNDER DOORMATS: MANDATING INSECURITY BY REQUIRING GOVERNMENT ACCESS TO ALL DATA AND COMMUNICATIONS (July 7, 2015), https://www.schneier.com/academic/paperfiles/paper-keys-under-doormats-CSAIL.pdf.

[43] Andrew Crocker & Gennie Gebhart, *Don't Let Encrypted Messaging Become a Hollow Promise*, ELEC. FRONTIER FOUND. (July 19, 2019), https://www.eff.org/deeplinks/2019/07/dont-let-encrypted-messaging-become-hollow-promise.

by chest or finger sensors.[44] This data is often logged and stored through a user's smartphone application, and may also be stored by a service provider's platform.

- *Smartwatch information:* smartwatches are similar to miniature smartphones, and contain many of the same sensors and instrumentation discussed in the smartphone section above. Many smartwatches are built to connect via Bluetooth to a nearby smartphone — and thus much of this sensor data may also be stored by the smartphone — but some have a built-in cellular chip to independently communicate with the user's cell service provider.
- *Other usage metadata:* the device may contain logs of other usage data, including connection history, battery heath information, and other data related to the operation of the device and its sensors. Much of this will be stored on the device, though the company's service carrier may gather and store some of this information for their continued development of these devices.

Notes and Cases:

- GPS tracking company Strava recently published a data set of location information drawn from assorted fitness devices who used their tracking application. A researcher reviewing that data discovered that it revealed the location of a number of military bases and other sensitive government locations, as personnel at those facilities wore fitness trackers while walking on the site.[45]
- A man in Connecticut has been charged with the murder of his wife, after evidence from the victim's FitBit was used to show that she had been active for more than an hour after the suspect had claimed that a third party had invaded their home and committed the murder.[46]

F. Home Assistant Devices

A growing number of people have purchased "smart speaker" or "home assistant devices," which allow a user to issue voice commands to an Internet-connected speaker to assist with a variety of tasks. Growth of the smart speaker market has been exponential, with an estimated 66.4 million owners in the United States.[47] *Examples:* Amazon Echo, Google Home, Apple HomePod.

Data Collected:

- *Ambient audio:* many of these devices are accessed through a voice command or "wake word" (e.g., "Alexa," "OK Google," "Hey Siri," etc.). This means the device must have a microphone on to hear the wake word, and thus may be in a position to record any other aural communications that happen while waiting for the "wake word." Based on current understandings, most researchers believe that these recordings are solely processed locally on the device itself, and are not stored in a permanently retrievable form.[48] It is perhaps possible that some of these ambient recordings could be retrieved, if they were made

---

[44] *See, e.g.*, Sharon Profis, *Do Wristband Heart Trackers Actually Work? A Checkup.*, CNET (May 22, 2014), https://www.cnet.com/news/how-accurate-are-wristband-heart-rate-monitors/.

[45] Zach Whittaker, *How Strava's "Anonymized" Tracking Data Spilled Government Secrets*, ZDNET (Jan 29, 2018), https://www.zdnet.com/article/strava-anonymized-fitness-tracking-data-government-opsec/.

[46] Dave Altimari, *All Evidence Turned Over As Fitbit Murder Case Moves Toward Trial*, HARTFORD COURANT (July 20, 2018), http://www.courant.com/news/connecticut/hc-news-fit-bit-murder-dabate-trial-20180720-story.html.

[47] Sarah Perez, *Over a Quarter of US Adults Now Own a Smart Speaker, Typically an Amazon Echo*, TECHCRUNCH (March 8, 2019), https://techcrunch.com/2019/03/08/over-a-quarter-of-u-s-adults-now-own-a-smart-speaker-typically-an-amazon-echo/.

[48] *See* Stacey Gray, *Always On: Privacy Implications of Microphone-Enabled Devices* at 5, FUTURE OF PRIVACY FORUM (April 2016), https://fpf.org/wp-content/uploads/2016/04/FPF_Always_On_WP.pdf.

very recently or the recordings were accidentally stored, but there are no reported examples of that happening.

- *Contents of commands:* after sending a "wake word" to the device, the device typically sends an audio recording of the contents of the communication to the device company's servers, in order to interpret the speech heard into a textual command and to process that command. Such records are likely stored on the server of the company afterwards as well, as such material would be useful for future development of the technology. It is also possible that contents of other communications are sent if the device mishears the "wake word" and begins to record.[49] Some companies — including Amazon[50] — make a history of your commands available to a user.
- *Usage metadata:* while documentation on this aspect of these services is sparse, it is likely that such devices record a variety of additional information around usage, including the date and time that commands are sent and device configuration information. It is likely that the service provider stores this information.

Notes and Cases:

- The first major test of use of information from a home assistance device was a murder case in Arkansas, where the victim was found in the suspect's house. When a witness testified that they remembered music coming from the suspect's Amazon Echo earlier in the night, police sought a search warrant against Amazon to have it provide any audio recordings and other usage data from the night in question. Amazon initially resisted, arguing that disclosing the suspect's listening and viewing information raises heightened First Amendment concerns.[51] The company later relented after the user gave consent. Late last year prosecutors dropped the case for lack of evidence.[52]
- There remains an open question as to how wiretapping laws in states (like Massachusetts[53]) that require consent from all parties to a communication apply to these sorts of devices. Devices frequently use some sort of visual cue that they are recording, such as a light that illuminates when activated, to help preserve arguments that those in the room at least constructively consented to such recordings. A class-action lawsuit was recently filed against Amazon, alleging that the Echo device's setup violates the Massachusetts wiretap act, along with the wiretapping laws of several other states.[54]

---

[49] Jay Stanley, *The Privacy Threat from Always-On Microphones Like the Amazon Echo*, ACLU (Jan. 13, 2017), https://www.aclu.org/blog/privacy-technology/privacy-threat-always-microphones-amazon-echo?redirect=blog/free-future/privacy-threat-always-microphones-amazon-echo

[50] *View Your Dialog History*, AMAZON, https://www.amazon.com/gp/help/customer/display.html?nodeId=201602040 (last visited July 17, 2018).

[51] Memorandum of Law In Support of Amazon's Motion to Quash Search Warrant, State v. Bates, No. Cr-2016-317-2 (Ark. Cir. Ct. Benton Cty. filed Feb. 17, 2017), *available at* https://regmedia.co.uk/2017/02/23/alexa.pdf (citing, *inter alia*, In re Grand Jury Subpoena to Kramerbooks & Afterwords, 26 Media Law Rep. 1599 (D.D.C. 1998); Tattered Cover, Inc. v. City of Thornton, 44 P.3d 1044 (Colo. 2002)).

[52] Nicole Chavez, *Arkansas Judge Drops Murder Charge in Amazon Echo Case*, CNN (Dec. 2, 2017), https://www.cnn.com/2017/11/30/us/amazon-echo-arkansas-murder-case-dismissed/index.html.

[53] Massachusetts prohibits "interception" of the contents of oral communications in many cases, with "interception" defined in the statute as, inter alia, "secretly record … the contents of any wire or oral communication through an intercepting device by any person other than a person given prior authority by all parties to such communication …." M.G.L. Ch. 272 § 99(B)(4). Commentators alternatively characterize this as an "all party consent" statute or a "secret recording" statute.

[54] Complaint, C.O. v. Amazon.com, Inc., No. 2:19-cv-910 (W.D. Wash. filed June 11, 2019).

G. In-Home "Internet of Things" ("IoT") Devices

Many new home appliances are Internet-enabled, and allow users to coordinate their operation through smartphone and desktop applications. To operate effectively these devices often will collect a wide array of usage data, which can be stored locally, on the user's smartphone, or with the manufacturer. *Example:* Google Nest, iRobot Roomba, Ring doorbell, Samsung Family Hub fridge.

Data Collected:

- *Sensory data: m*ost IoT devices rely on sensory data of some form in order to operate — a Nest doorbell will use a camera to track motion, a Roomba vacuum will use location and laser-based location detection ("LiDAR") to map out the room, a Nest will measure room temperature, and so forth. This data is often logged, and frequently shared with the relevant service provider, and is sometimes made available to a user for control or inspection of performance.
- *Operational instructions:* users can send specific configuration instructions to IoT devices, which are then stored on the device, on the user's smartphone, and likely stored by the service provider in question. This may include operating parameters and configuration information, which depending on the device may provide additional information about what the user is doing with the device, as well as information concerning the user's Wi-Fi connection, including their Wi-Fi router's device ID and password.
- *Usage history:* most IoT devices log information regarding their past performance, which could then be used to determine what the user was doing with the relevant device. This information is likely stored on the device, as well as transmitted to the service provider.

Notes and Cases:

- In the same Arkansas murder case discussed above, law enforcement sought information from the platform for the suspects Internet-enabled water meter, which they claimed would show an unusual amount of water use the night of the murder.[55]
- In a report in February 2018, journalist Kashmir Hill and technologist Surya Mattu examined how frequently home "Internet of Things" devices transmit data back to their servers, and what one could do with that information. The report found that devices sent traffic back to their servers at fluctuating times based on usage, which could then be used to make inferences about its activity. For example, Mattou was able to show that Hill stayed home on New Years Eve, because her television was sending a higher level of data back to its carrier, suggesting that it was on.[56]

---

[55] Kathryn Gilker, *Bentonville Police Use Smart Water Meters As Evidence In Murder Investigation*, KFSM (Dec. 28, 2016), https://5newsonline.com/2016/12/28/bentonville-police-use-smart-water-meters-as-evidence-in-murder-investigation/.

[56] Kashmir Hill & Surya Mattu, *The House The Spied On Me*, GIZMODO (Feb. 7, 2018), https://gizmodo.com/the-house-that-spied-on-me-1822429852.