BRENNAN CENTER FOR JUSTICE

Government Access to Mobile Phone Data for Contact Tracing

A Statutory Primer

By Harsha Panduranga and Laura Hecht-Felella with Raya Koreh PUBLISHED MAY 21, 2020

In an effort to contain the coronavirus, companies and governments across the globe are developing technological tools to trace its spread. Many of these tools seek to monitor individuals and groups in order to help identify potential carriers of the virus, alert people who may have been infected, flag places that may be at high risk, and measure the impact of public health initiatives such as social distancing directives. While proposals run the gamut from analyzing networked thermometer data nationwide to deploying remote heat sensors for fever detection,[1] in the U.S. attention is focused mostly on using location or proximity data produced by cell phones to track movements and interactions at both the individual and population levels.[2]

Many of these tools are being developed by the private sector, but the federal government and state governments are clearly interested in influencing their design and accessing the data they generate.[3] At the same time, the patchwork of laws governing the disclosure of location data to the government — by cell phone companies, smartphone application developers, data brokers, individuals, and others — does not adequately protect Americans' privacy. Cell phone carriers are fairly heavily regulated when it comes to individually identifiable data, but constraints on other entities that collect similar information are markedly weaker. Aggregate data that does not explicitly divulge individuals' locations, identities, or associations is subject to even fewer limitations, despite evidence that it can sometimes be disaggregated and de-anonymized.[4]

Moreover, there are few limits on the sharing of location information among government agencies.[5] Instead, several laws promote government-wide information sharing.[6] For example, location data collected by the U.S. Department of Health and Human Services (HHS) for the ostensible purpose of combating the coronavirus might easily be shared with local governments, other federal agencies, or law enforcement.[7]

Any effort to use location or proximity tracking must compensate for the lack of a regulatory framework that protects Americans' civil liberties. As the Supreme Court has repeatedly recognized, location information can reveal intimate details of a person's life, including visits to a lawyer, psychiatrist, specialized health clinic, or religious site.[8] Absent meaningful safeguards, government collection of revealing information might infringe on core civil liberties such as freedom of association and freedom of expression, especially if the data is misappropriated.

The government's use of location or proximity data also raises equity concerns. In the United States, one out of every five adults does not own a smartphone — with older and low-income Americans representing a disproportionate share of those without such a device.[9] Using location data to inform a government response to the coronavirus will be less effective and less successful due to these gaps. On the flip side, inequities might also be manifested if measures of aggregate foot traffic generated by cell phone location data are used to calibrate the enforcement of social distancing measures. Communities where people move around more because they must commute to a job, need to travel farther to buy groceries, or are looking for shelter may become targets of outsize policing.[10]

Statutory Overview

There is no comprehensive data privacy law in the United States; instead, a piecemeal statutory structure protects certain types of personal data.[11] The Stored Communications Act (SCA) and the Telecommunications Act are most relevant to the question of when private companies may voluntarily disclose location data (revealing where a person is) or proximity data (revealing how close a person is to another) to the government. Together, these two laws limit companies providing certain services to the public from voluntarily revealing an individual's personally identifiable location or proximity information to the government, whether it originates from cell tower data, GPS, Bluetooth, Wi-Fi, a combination of these sources, or some other source entirely.

Specifically, the SCA prohibits entities that provide phone, messaging, data storage, or data processing services to the public from voluntarily disclosing to the government the content of communications they carry or maintain, or their customer's records.[12] Whether location or proximity data might be categorized as "content" or a "record" within the meaning of the SCA is a fact-specific question that depends in part on the purpose for which it is logged or transmitted, as described in further detail below.[13] The Telecommunications Act prohibits phone carriers from disclosing their customers' personally identifiable call location information to any entity, including the government and data brokers.[14]

The Federal Trade Commission (FTC) Act might also protect Americans where companies have violated promises not to disclose particular types of data. But it can only be enforced by the federal government itself, which is unlikely to happen where it is the federal government seeking the data (see sidebar on p. 5). The main types and sources of location and proximity data, as well as the relevant governing statutes, are outlined in the appendices to this report.

Whether each statute prohibits the disclosure of location or proximity data to the government depends on a number of factors. There are a number of key considerations:

- Have people opted into an application or other program through which they know data may be shared with the government for the purpose of combating the coronavirus?
- If not, does a company with this data have its customers' consent to disclose it?
- In what capacity was a wireless carrier, a developer of a smartphone application or platform, a data broker or analytics provider, or another source acting while collecting the data? For example, was the entity providing messaging, data storage, or data processing services?
- Is the data aggregated in a fashion that makes it impossible to connect to individuals?
- Has the data been sufficiently de-identified? That is, have individual data points been stripped of details — such as a name, phone number, or address — that would make them immediately linkable to a given person?

Gaps in this regulatory framework permit workarounds for governments seeking people's location or proximity data without their knowledge or consent. For example, while the government could not get an individual's location information from a cell service provider, such as AT&T or Verizon, without a warrant,[15] it may be able to buy it from a data broker who is legally able to purchase similar information from a smartphone application developer who collects it. Constitutional arguments, not discussed here, may provide fodder for additional constraints.[16]

Tracking Initiatives

Proposals to mitigate the spread of the coronavirus through phone location or proximity data have emerged from a range of sources, including academic institutions, for-profit companies, and governments. This primer divides discussion of these proposals into two categories: individualized and aggregate data.[17]

Individualized data is linked to a specific person who is sometimes identified by details such as name, phone number, or specific smartphone. For instance, location data revealing the path of an individual diagnosed with the coronavirus over the past 14 days, which might be used to determine whom she could have infected, is a type of individualized data.

In contrast, aggregate data collects, combines, and communicates information in terms of totals, summaries, or statistics, rather than in reference to a specific individual.[18] The percentage decrease of people at a waterfront park after implementation of social distancing protocols is an example of aggregate data.

Individualized Data

Proposals deploying individualized location or proximity data to fight the coronavirus aim to use the information for a range of purposes: to track the paths of people who are infected with the virus in order to identify those might have been exposed to it (a process known as contact tracing or exposure notification), to pinpoint disease hot spots, to model infection rates and spread, or to inform public health decisions.[19] Many such proposals would use location data that reveals where an identified person was or is at a given point in time. Some contact tracing proposals would track proximity rather than location, using Bluetooth technology to determine when two people have been close enough to each other for enough time to enable transmission. This information might be stored on a central server or decentralized on local devices. The proximity-based proposals that are gaining traction in the United States are designed to be anonymous: they would make it difficult to link a person's identity with their proximity history or diagnosis, and they would rely on a decentralized process to match contacts.

As a general matter, both location-based and proximity-based proposals in the United States contemplate asking people to voluntarily download smartphone applications that would solicit user consent for information sharing and take some steps to protect user privacy. These apps vary with respect to their features, mechanics, and privacy measures. Many are or will be run by governments, but they need not be. Nonetheless, there is a debate both in the U.S. and overseas about whether a voluntary system can achieve the levels of adoption necessary to be effective, or whether compulsory approaches that do not require user knowledge or consent are better suited to combat the virus.

One category of voluntary proposals — location-based programs — would use GPS and Bluetooth technologies to create and store an encrypted, time-stamped log of where a user has been over the past month.[20] People who test positive for the coronavirus can choose to share this log with health officials, who may then use it to help patients jog their memory about where they had been and with whom they may have come in contact. Some platforms, such as MIT's Private Kit: Safe Paths, use "overlapped GPS and Bluetooth trails" to allow healthy app users to check — against location data logged locally on their phones — if they may have crossed paths with someone who has tested positive for the disease and chosen to share their data with public health officials for dissemination in an "anonymized, redacted, and blurred" form.[21] Without further details, however, it is unclear whether patients could be re-identified with relative ease.[22] According to a spokesperson for MIT's Private Kit, three local governments in the U.S. plan to use the app, and 17 more are considering doing so.[23] Utah and North Dakota have confirmed rollouts of apps that incorporate location-based functionalities similar to those described here, though it is unclear whether they are built on Private Kit or the extent to which they are decentralized.[24]

Another category of voluntary proposals would use individual data for proximity tracking. Apple and Google recently announced a joint effort to allow applications on Apple's iOS and Google's Android platforms — whether created by governments or private companies associated with public health authorities — to use Bluetooth technology for exposure notification.[25] These applications would enable phones close to each other for a period of time to log that contact by exchanging anonymous identifier keys, sent directly from phone to phone in a decentralized model. A user who later tested positive for the coronavirus could enter a code that would upload 14 days' worth of proximity keys to a cloud server. The server would then push those keys to other app users' phones, which would check to see if there was a match.[26] Since the transmitted keys would be randomized and change intermittently, and because they would be generated at great volume, it would be difficult to associate a key with

a particular phone. Some contact tracing apps that use location-based data, such as Care19, an application developed by the North Dakota Department of Health in partnership with ProudCrowd, also incorporate this proximity-based technology.[27]

So far, it appears that Apple and Google would require that developers decentralize matches, meaning matches would be confirmed on an individual's phone rather than on a central server.[28] Other Bluetooth proximity-tracking applications have varying levels of privacy protections. For example, Singapore's TraceTogether permits authorities to know user identities and makes matches of potential contacts centrally, and the UK's National Health Service plans to implement a similar program.[29]

Further Uses of Location Information

Some of the apps described here would use location information collected with users' consent for purposes other than direct contact tracing. For example, North Dakota's app says the data will help identify places with clusters of people who test positive for the coronavirus so it can "more proactively act to reduce the rate of spread," as well as model infection rates and health-care demand.[30]

Programs in Israel and South Korea are more coercive. In March, Israel's Health Ministry began using individual, identifiable cell phone location data, initially funneled from wireless carriers to a counterterrorism database, to map where people known to have the coronavirus had been over the previous two weeks and ascertain with whom they might have crossed paths.[31] Those who could have been exposed were sent a text and told to self-isolate.[32] The monitoring was done without securing customer consent. At the end of April, Israel's Supreme Court ruled that if the government wanted to continue tracking people's phones, it had to bring the program under legislation within the coming weeks.[33]

A similar effort in South Korea operates under the authority of the country's Infectious Disease Control and Prevention Act, which allows health officials to use phone location information with the permission of law enforcement and other government stakeholders.[34] The program relies on phone GPS data, along with sources like credit card records, to map the paths of confirmed cases, making these routes public or accessible to those in the region at a level of detail that has been sufficient to identify the infected person.[35] This has resulted in the harassment and stigmatization of some of those identified as positive for the virus.[36]

Aggregate Data

Some virus response efforts contemplate drawing aggregate location data from a large number of cell phones, with the goal of discerning population-level trends rather than the movement of any particular individual. This information can help policymakers assess compliance with social distancing orders and map the spread of the disease. News reports indicate that mobile advertising companies are sharing such data with the U.S. Centers for Disease Control and Prevention (CDC), as well as with state and local governments, to display the degree to which people are congregating in public places, going shopping, or moving from one place to another.[37]

The federal government has also reportedly been in discussions with large tech companies, including Google and Facebook, on how it can use aggregated location data for these purposes.[38] For example, Google is using aggregated data culled from users who have enabled the location history setting on their Google account to track movement trends.[39] This project, called COVID-19 Community Mobility Reports, is intended to help public health officials make decisions about transportation to certain high-volume destinations, business hours, and guidance regarding essential trips and deliveries. The mobility reports display a percentage point increase or decrease in the number of visits to a location but not the absolute number of visits. Apple has announced it is doing something similar with Apple Maps data.[40]

Applicable Statutes

This section evaluates the degree to which relevant statutes — namely, the Stored Communications Act (SCA) and the Telecommunications Act — limit companies' *voluntary* disclosure of individualized location or proximity data to the government.[41] Though the statutory landscape is rapidly evolving — for example, two Covid-19-related data privacy bills were introduced in the Senate in May[42] — it does not seem that the SCA or the Telecommunications Act significantly constrain any of the U.S. proposals in their current form, for two reasons.

First, current proposals to use individualized data involve people granting permission to the government to collect and use their information, against which there is no legal bar.[43] A conceivable scenario down the road, though, is one in which a privately administered app — using the Private Kit template, for example — gives location or proximity information it has logged to the government without authorization from its users.[44] If this information — arguably protected as "content" or a "record or other information" under the SCA[45] — is stored or processed remotely by the application, the SCA may restrict disclosure.[46] In contrast, the decentralized Apple/Google proposal is restricted to use by public health authorities; users who volunteer to share their diagnosis keys would be agreeing to share this information with the government.[47] Since proximity keys would be stored locally, on individual phones rather than in a central database, there would be little else of value for the government to collect.

Second, with respect to the proposals to use aggregate data, there are few legal limitations on private companies' voluntarily disclosing aggregate cell phone location data to the government. For example, the Telecommunications Act affirmatively allows wireless carriers, such as Verizon and AT&T, to disclose aggregate customer information when "individual customer identities and characteristics have been removed."[48] While the SCA prohibits companies such

The Federal Trade Commission Act

The Federal Trade Commission (FTC) Act applies to companies that collect or maintain location data, such as Google, Apple, Facebook, Twitter, and Uber, and to data brokers that compile consumers' personal information and resell or share that information with others.[49] It also applies to the privacy practices of phone providers, such as Verizon, AT&T, and T-Mobile, though its jurisdiction over these common carriers is much more limited.[50] The FTC does not, however, have jurisdiction over most nonprofit organizations, including many universities, which have been proposed as trusted organizations through which to run contact tracing programs.

Unlike the SCA and the Telecommunications Act, the FTC Act does not impose additional regulations on companies' disclosure of customer information. Rather, the act holds companies to the privacy commitments they have made to their customers. Under Section 5 of the act, the FTC can investigate and bring enforcement actions to hold companies accountable for misleading privacy policies,[51] including those pertaining to location data, which it has recognized as sensitive information that implicates significant privacy concerns.[52] Notably, some of the companies reportedly in discussion with government entities regarding sharing of location information, such as Google and Facebook,[53] are already under consent decrees with the FTC for privacy lapses.[54] For example, the FTC recently announced that Facebook would pay a $5 billion penalty and agree to a 20-year settlement order to resolve allegations that the company deceived users about their ability to control their personal information using Facebook's privacy settings.[55]

As seen in the Facebook example, the act might facilitate meaningful privacy protections for individuals' data. However, companies that collect or maintain location data — including operating systems like Google's Android and Apple's iOS, phone applications like Facebook and Twitter, and data brokers — tend to have privacy policies that distinguish between identifiable and nonidentifiable data. Their policies generally explicitly permit disclosure of nonidentifiable data to third parties,[56] so the FTC is unlikely to provide a barrier to the disclosure of anonymized, aggregated data.

Moreover, the FTC Act has no private right of action, meaning that individuals cannot seek a remedy under it; instead, the federal government would have to enforce any violation of the act. Where the federal government is the one seeking disclosure in a time of crisis, it is unlikely to turn to the act to halt its own data-solicitation practices. However, the act could perhaps be a tool to deter organizations administering digital coronavirus containment programs from selling the data they collect to private actors or disclosing it to state and local governments.

as Facebook, Gmail, and YouTube, in the course of providing public messaging, data storage, or data processing services,[57] from voluntarily disclosing their customer records to the government, it does not explicitly address aggregate data. Notably, the Department of Justice has interpreted the act to permit the disclosure of aggregate records as long as they do not "identify or otherwise provide information about a particular subscriber or customer."[58]

For more coercive contact tracing initiatives that use individualized, identifiable data without explicit consent, such as those from Israel and South Korea, the legal framework is largely dependent upon the type of service a company provides to the public:[59]

- **Wireless carriers.** The SCA and the Telecommunications Act prohibit wireless carriers like Verizon, AT&T, or Sprint from disclosing individualized call location data to the government without a warrant or other legal authorization.[60]

- **Smartphone app developers and platforms.** Whether the SCA covers developers of smartphone applications that collect location data depends on whether they collect that data in the course of providing messaging, data storage, or data processing services. Social media services like Facebook or Twitter and email clients like Gmail have been found to be covered when they serve primarily to allow people to exchange and store messages.[61] Services that mainly let users upload and store or process content, such as YouTube or DropBox, may also be covered.[62] So too may services that exist for the purpose of logging a person's location — for example, Google's Location History function.[63] The same rules apply to built-in functionalities of smartphone operating systems, such as iMessage or iCloud in Apple's iOS.[64]

- **Data brokers.** If the U.S. government were looking to implement a tracking initiative like Israel's or South Korea's, it might approach firms that buy or otherwise obtain location data to aggregate and resell it to other parties, to provide analytics to optimize advertising or other functions, or for some other reason. The SCA does not prohibit these companies from disclosing their data to the government.[65]

  This is not a complete workaround, though. Wireless carriers and other companies that collect location data may be held accountable in other ways for the downstream consequences of selling or sharing the data with third-party data brokers. For example, in February 2020 the Federal Communications Commission (FCC) formally proposed fining AT&T, Sprint, T-Mobile, and Verizon more than $200 million for disclosing customer location data through a chain of third-party brokers to law enforcement in violation of the Telecommunications Act.[66] The enforcement notice highlighted how the wireless carriers had failed to safeguard customers' information as it was transmitted to aggregators that sent it to companies providing location-based services — navigation, local weather, or fraud prevention, for example. The carriers were alleged to be responsible for the downstream unauthorized disclosure of customers' location data to a state sheriff's office. It is also possible that the SCA would prohibit a wireless phone company or other entity providing a covered service from selling location data directly to an aggregator or broker with the knowledge that the government would eventually get it, though this has not been tested in court.[67]

As described above, user consent and voluntary adoption are key components of the proposals currently being considered in the United States. Both the SCA and the Telecommunications Act contain user-consent exceptions to their prohibitions on the disclosure of identifiable information. More coercive proposals, in which companies would voluntarily disclose identifiable data without user consent, might implicate the statutes' emergency exceptions.

Consent

The SCA and the Telecommunications Act, as well as FCC regulations implementing the Telecommunications Act, explicitly require customers to consent to the disclosure of identifiable data.[68] Without specific customer consent for the disclosure of location or proximity data, or a privacy policy permitting the practice, it is unlikely that courts would find that people have legally consented to the disclosure of this data to the government in order to operationalize a location-based contact tracing proposal mapping out individuals' travels, akin to South Korea's.[69] We reviewed privacy policies and terms-of-service agreements governing customer-provider relationships from some major companies, including wireless carriers (Verizon and AT&T), a social media company (Facebook), and tech companies (Apple and Google).[70] Notably, none could reasonably be read to permit the blanket disclosure of user data to the government, though it is unclear to what degree that finding is generalizable to the industry as a whole.[71]

Emergencies

The emergency exception of the SCA could conceivably be invoked in support of coronavirus containment measures involving contact tracing. Under the SCA, a provider using the exception needs to believe in good faith (1) that there is an emergency involving danger of death

or serious physical injury to any person, (2) that it requires disclosure of information without delay, and (3) that the information relates to the emergency. Historical uses have included locating a missing person thought to be imminently at risk of harm and tracking a suspect fleeing a crime who is believed to pose an imminent danger to others.[72] The Telecommunications Act's emergency exception is narrower, focusing on facilitating 911 services and permitting the disclosure of information to family members when an individual is in a "situation that involves the risk of death or serious physical harm."[73] Although these exceptions have not been used in the past to permit something like widespread contact tracing, they could be invoked now if the government asks companies to provide location data voluntarily in light of the severity of the public health crisis and the exponentially increasing costs of delaying action.[74]

Conclusion

Proposals that would map individuals' movements for disease-tracking purposes in the U.S. — in contrast to many other countries — have so far envisioned voluntary rather than compulsory participation. If individuals decide to share their data, the information can be used in accordance with the terms of that disclosure.

However, digital contact tracing or exposure notification needs a high rate of nationwide buy-in to work, and policymakers looking to avoid the continuation of broad lockdowns will be looking for ways to increase participation and data collection as the coronavirus pandemic continues. The statutory law outlined in this primer will be most applicable in such scenarios. As proposals are developed, it is essential that they include privacy protections for users given the significant gaps in the statutory framework, particularly regarding the disclosure of information to third parties and the disclosure of aggregate data. This crisis has made clear the need for strong, reliable protections for the privacy and security of personal data, especially the highly sensitive health and location information resulting from testing and contact tracing.

Appendix 1

SOURCES OF LOCATION AND PROXIMITY DATA	
Cell towers	Cell phones connect to nearby cell towers several times a minute when they are turned on. Each connection generates a time-stamped record containing the identity of the phone and location of the cell tower. This data, which can be used to determine a cell phone's approximate location, is called cell-site location information (CSLI) and is stored by some phone providers for up to five years.[75]
Global Positioning System (GPS)	Some cell phones contain a GPS chip, which generates location information by calculating its distance from four or more of the GPS satellites orbiting Earth.[76] This data may be stored locally on a device or transmitted to a central database.
Bluetooth	Some cell phones contain a Bluetooth chip, which continuously broadcasts probe signals using short-range radio when it is turned on. As these signals are received by nearby Bluetooth devices, they can be used to generate proximity information. Signals received by fixed Bluetooth beacons can also be used to generate location information.[77]
Wi-Fi	It is possible to approximate the location of a cell phone by tracking its unique hardware identifier, called a Media Access Control (MAC) address, as it connects to nearby Wi-Fi networks.[78]

Appendix 2

STATUTES GOVERNING DISCLOSURE OF LOCATION AND PROXIMITY INFORMATION				
	Stored Communications Act (SCA) (18 U.S.C. § 2702)	**Telecommunications Act (47 U.S.C. § 222)**	**Federal Trade Commission (FTC) Act (15 U.S.C. § 45)**	**Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule (45 C.F.R. §§ 160 and 164)**
Summary	The SCA prohibits entities that provide phone, messaging, data storage, or data processing services to the public from voluntarily disclosing the content of communications they carry or maintain, as well as customer records or information in connection with their provision of those services. Disclosure of proximity or location information to any third party, whether to the government or to a private data broker from which the government can buy it, may be prohibited if it is considered the "content" of a communication under the SCA. If it is a "record or other information" connected to a customer, disclosure to the government is barred but the data may be shared with other third parties.[79] Whether location information is categorized as "content" or a "record" is a fact-specific question that depends in part on the purpose for which it is collected or transmitted.[80] The SCA probably restricts the disclosure of de-identified data tied to discrete individuals, even if it is transmitted in bulk.[81] Court decisions bearing on the SCA's application to the proposals of concern to this primer have considered location — as opposed to proximity — information.	The Telecommunications Act prohibits phone carriers from disclosing their customers' personally identifiable call location information to any entity, including the government or data brokers.[82] The degree to which it prohibits the disclosure of de-identified information disclosed in bulk is unclear.[83]	The FTC Act prohibits companies that collect or compile customer data, such as social media sites, online stores, or data brokers, from deceiving or misleading consumers about their privacy policies. The FTC enforces this provision by investigating and bringing enforcement actions against companies that have misrepresented their privacy policies.[84] The FTC Act has been enforced against companies for improperly disclosing customers' location data.[85] There is no reason to think the unauthorized disclosure of proximity data would be treated differently than that of any other customer data.[86]	The HIPAA Privacy Rule provides national standards that define and restrict the ability of health-care providers and their associates to save, access, and share individuals' medical records and other individually identifiable health information.[87] The HIPAA Privacy Rule does not meaningfully restrict disclosure of aggregate data, de-identified data, or non-health information.[88]

	Stored Communications Act (SCA) (18 U.S.C. § 2702)	Telecommunications Act (47 U.S.C. § 222)	Federal Trade Commission (FTC) Act (15 U.S.C. § 45)	Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule (45 C.F.R. §§ 160 and 164)
Covered entities or activities	The SCA's coverage[89] has been found to include ■ Verizon, Sprint, AT&T, T-Mobile, and other phone carriers;[90] ■ Facebook, Dropbox, Gmail, and other companies when providing social media messaging, storage, or email services;[91] and ■ YouTube and other companies when providing services that permit users to upload content.[92] The SCA may apply to cell phone operating systems, such as Apple's iOS and Google's Android, to the extent they provide messaging, data processing, or data storage services.[93] The SCA likely does not apply in cases where the primary purpose of a service at issue is not best characterized as storage, processing, or messaging. For example, where companies like eBay or Amazon provide such features in a manner incidental to their retail or auctioneering functions, the SCA has been found not to apply.[94]	The act applies to wireless carriers, such as Verizon, Sprint, AT&T, and T-Mobile, and any other providers of telecommunications services.[95]	The act gives the FTC the authority to regulate most "persons, partnerships, or corporations,"[96] including ■ companies that collect or maintain location data, such as Google, Apple, Facebook, Twitter, other cell phone applications, and online stores; and ■ data brokers that compile consumers' personal information and resell or share that information with others.[97] The FTC has limited jurisdiction over "common carriers" like Verizon, AT&T, and T-Mobile, though the FTC can regulate their privacy practices.[98] It cannot enforce the FTC Act against most nonprofit organizations.[99]	HIPAA's coverage includes health plans, health-care clearinghouses, most health-care providers, and business associates and subcontractors of those entities that create, receive, maintain, or transmit protected health information.[100] Business associates of covered entities can include medical billing agencies, accountants, and IT consultants, as well as tech firms that help hospitals manage and analyze patient data.

	Stored Communications Act (SCA) (18 U.S.C. § 2702)	Telecommunications Act (47 U.S.C. § 222)	Federal Trade Commission (FTC) Act (15 U.S.C. § 45)	Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule (45 C.F.R. §§ 160 and 164)
Covered data	Companies providing covered services are generally prohibited from voluntarily disclosing a customer's "record or other information" to the government.[101] There is no definition of "record" in the statute, but courts have interpreted the term to include some data revealing a customer's location, most notably cell-site location data.[102] Location data may also be considered the "content" of a communication, especially if the purpose of a service is to record or communicate it. For instance, Google has argued that its Location History feature acts as a journal logging a person's whereabouts, with the retained data therefore being the "content" of an entry.[103] Disclosure to any third party is prohibited when location data is "content."	Covered companies are generally prohibited from disclosing customer proprietary network information (CPNI), which explicitly includes a customer's location information logged in connection with making or receiving a call.[104]	Covered companies are prohibited from engaging in "unfair or deceptive acts or practices,"[105] which would include false or misleading privacy policies pertaining to location or proximity data.[106]	The HIPAA Privacy Rule covers "protected health information" — patients' medical records and other individually identifiable health information — in paper and electronic formats.[107]

	Stored Communications Act (SCA) (18 U.S.C. § 2702)	Telecommunications Act (47 U.S.C. § 222)	Federal Trade Commission (FTC) Act (15 U.S.C. § 45)	Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule (45 C.F.R. §§ 160 and 164)
Prohibitions on disclosure	As described above, entities may be barred from voluntarily sharing customer location data obtained in the course of providing phone, messaging, data storage, or data processing services, unless an exception applies, such as customer consent or an emergency. Absent consent given for a discrete purpose, courts may look to privacy policies and terms-of-service contracts to determine whether a disclosure was authorized. The emergency exception applies if the provider believes in good faith (1) that there is an emergency involving danger of death or serious physical injury to any person, (2) that it requires disclosure of information without delay, and (3) that the information relates to the emergency.[108] The SCA does not specifically address the disclosure of de-identified or aggregate data. However, the U.S. Department of Justice has interpreted the act to permit companies to voluntarily disclose to the government aggregated data "that does not identify or otherwise provide information about a particular subscriber or customer."[109]	Covered companies are barred from disclosing CPNI to any other entity unless an exception applies, such as customer consent or an emergency.[110] Companies can disclose aggregate customer information, defined as data that relates to a group of customers and from which individual identities and characteristics have been removed.[111]	Companies that engage in "unfair and deceptive acts," including data collection, use, and sharing practices that contradict the commitments they have made to their customers, may become the target of FTC investigations or enforcement actions.	In general, protected health information may be used or disclosed as necessary without patient consent for the purposes of delivering treatment,[112] seeking payment, or running health-care operations only. Aside from those purposes, entities are barred from voluntarily sharing protected information unless an exception applies, such as to prevent or control disease[113] or to prevent or lessen a serious and imminent threat to the health and safety of a person or the public.[114] During the Covid-19 emergency, business associates of covered entities — such as billing agencies or IT consultants — can make good-faith use of and disclose protected health information for public health activities without penalty.[115]

Endnotes

1 See, e.g., Ed Garsten, "Drive-By Heat Sensors Could Help Detect Vehicle Occupants with COVID-19," *Forbes*, April 1, 2020, https://www.forbes.com/sites/edgarsten/2020/04/01/drive-by-heat-sensors-could-help-detect-vehicle-occupants-with-covid-19/#455a60b62b0e; "Taking People's Temperatures Can Help Fight the Coronavirus," *Economist*, March 26, 2020, https://www.economist.com/science-and-technology/2020/03/26/taking-peoples-temperatures-can-help-fight-the-coronavirus; and Donald McNeil Jr., "Can Smart Thermometers Track the Spread of the Coronavirus?," *New York Times*, March 18, 2020, https://www.nytimes.com/2020/03/18/health/coronavirus-fever-thermometers.html.

2 This primer focuses on location data obtained through cell phones, though such data may also be gleaned from other surveillance technologies, like video, facial recognition, or automated license plate readers. See, e.g., Caroline Haskins and Ryan Mac, "A US Senator Wants to Know Which Federal Authorities Are Using Clearview AI to Track the Coronavirus," *BuzzFeed News*, April 30, 2020, https://www.buzzfeednews.com/article/carolinehaskins1/senator-markey-clearview-ai-covid-contact-tracing; and Catherine Crump, *You Are Being Tracked: How License Plate Readers Are Being Used to Record Americans' Movements*, American Civil Liberties Union, July 2013, https://www.aclu.org/issues/privacy-technology/location-tracking/you-are-being-tracked.

3 Elliot Setzer, "Contact-Tracing Apps in the United States," *Lawfare*, May 6, 2020, https://www.lawfareblog.com/contact-tracing-apps-united-states; Ryan Browne, "How Governments and Big Tech Are Looking to Curb the Spread of Coronavirus with Your Smartphone," CNBC, April 16, 2020, https://www.cnbc.com/2020/04/16/coronavirus-apple-google-and-governments-using-contact-tracing-tech.html; and *Enlisting Big Data in the Fight Against Coronavirus: Hearing Before the Senate Committee on Commerce, Science, and Transportation,* 116th Cong. (2020), https://www.commerce.senate.gov/2020/4/enlisting-big-data-in-the-fight-against-coronavirus.

4 Although aggregate data conveys information about groups rather than individuals, it may be possible to identify individuals, especially if the data refers to a small geographic area or group, or if it is combined with publicly available information and examined over time. See Sidney Fussell and Will Knight, "The Apple-Google Contact Tracing Plan Won't Stop Covid Alone," *Wired*, April 14, 2020, https://www.wired.com/story/apple-google-contact-tracing-wont-stop-covid-alone; Ling Yin et al., "Re-Identification Risk versus Data Utility for Aggregated Mobility Research Using Mobile Phone Location Data," *PLoS ONE* 10, no. 10 (2015), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4607417; Ed Felten, "Is Aggregate Data Always Private?," *Tech@FTC Blog*, Federal Trade Commission, May 21, 2012, https://www.ftc.gov/news-events/blogs/techftc/2012/05/aggregate-data-always-private; and Joseph A. Calandrino et al., "'You Might Also Like:' Privacy Risks of Collaborative Filtering," *IEEE Symposium on Security and Privacy* (May 2011): 231–246, http://www.cs.utexas.edu/~shmat/shmat_oak11ymal.pdf.

5 Neither the Privacy Act of 1974 nor the Health Insurance Portability and Accountability Act (HIPAA) provides sufficient protection against information sharing. The Privacy Act, which protects records about individuals retrieved by personal identifiers like name or date of birth, does not apply to aggregate or anonymized location data, or databases that contain personally identifiable information but do not retrieve information using that data. Moreover, the act contains substantial exceptions, including permitting information sharing with law enforcement and disclosures for "routine uses," which agencies often reserve when giving notice of a data collection proposal. Privacy Act of 1974, 5 U.S.C. § 552a (2020); Privacy of Individually Identifiable Health Information, 45 C.F.R. §§ 164.500 to 164.534 (2019). Similarly, HIPAA, which establishes the conditions by which a health-care provider or associate may disclose individually identifiable health information, does not meaningfully restrict disclosure of aggregate or de-identified data or non-health information. In addition, in light of Covid-19, HHS recently released a waiver that significantly curtails the scope of HIPAA protections and facilitates information sharing. See Office of the Secretary, U.S. Department of Health and Human Services, "Enforcement Discretion Under HIPAA to Allow Uses and Disclosures of Protected Health Information by Business Associates for Public Health and Health Oversight Activities in Response to COVID–19," *Federal Register* 85, no. 67 (April 7, 2020), https://www.govinfo.gov/content/pkg/FR-2020-04-07/pdf/2020-07268.pdf.

6 For example, the National Counterterrorism Center (NCTC) is directed by statute to "ensure that agencies . . . have access to and receive all-source intelligence support needed to execute their counterterrorism plans or perform independent, alternative analysis" and to ensure that such agencies "have access to and receive intelligence needed to accomplish their assigned activities." 50 U.S.C. § 3056 (2020). A recent memorandum written by U.S. Deputy Attorney General Jeffrey Rosen designating the coronavirus as a "biological agent" means that information collected by government health officials to counter the coronavirus might be shared with other agencies and law enforcement within the NCTC. See Jeffrey Rosen, U.S. Deputy Attorney General, to All Heads of Law Enforcement Components, Heads of Litigating Divisions, and United States Attorneys, memorandum, March 24, 2020, Department of Justice Enforcement Actions Related to COVID-19, https://www.justice.gov/file/1262771/download.

7 Within HHS, data sharing practices vary widely. In a 2018 report, the agency noted: "The Department lacks a consistent, transparent, and standardized framework for sharing restricted and nonpublic data among its agencies in a timely and efficient manner. Each agency, and often agency personnel for each dataset, has the autonomy to interpret the rules for data sharing processes. Data sharing processes can range from non-existent and informal, to formal and consistent. . . . The data governance rules are not formalized. The sharing of those datasets can be ruled by individual relationships and/or staff availability." Office of the Chief Technology Officer, U.S. Department of Health and Human Services, *The State of Data Sharing at the U.S. Department of Health and Human Services*, September 2018, https://www.hhs.gov/sites/default/files/HHS_StateofDataSharing_0915.pdf. One significant concern is that location data collected by HHS or another government agency might eventually find its way into the hands of law enforcement, which would ordinarily be required to obtain a warrant or court order before obtaining such data. Both the Privacy Act and HIPAA Privacy Rule contain exceptions for disclosures to law enforcement. 5 U.S.C. § 552a (2020); 45 C.F.R. §§ 164.500 to 164.534.

8 Several recent U.S. Supreme Court decisions regarding Fourth Amendment protections for location data have highlighted the sensitivity of this information. For example, the U.S. Supreme Court noted in *Carpenter v. United States* that location data reveals a wealth of detail about a person's "familial, political, professional, religious, and sexual associations." Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018). In *United States v. Jones,* Justice Sotomayor discussed that disclosed in location data will be things that are indisputably private in nature — including "trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on." United States v. Jones, 132 S. Ct. 945, 955 (2012) (Sotomayor, J., concurring) (quoting People v. Weaver, 12 N.Y.3d 433, 441–442 (N.Y. 2009)).

9 "Mobile Fact Sheet," Pew Research Center, June 12, 2019, https://www.pewresearch.org/internet/fact-sheet/mobile.

10 Amos Toh, "Big Data Could Undermine the Covid-19 Response," *Wired*, April 12, 2020, https://www.wired.com/story/big-data-could-undermine-the-covid-19-response.

11 Zachary S. Heck, "A Litigator's Primer on European Union and American Privacy Laws and Regulations," *Litigation* 44, no. 2 (2018): 59 ("The United States has a patchwork of laws at both the federal and state levels relating to data protection and information sharing.").

12 The Stored Communications Act (SCA) prohibits covered entities from knowingly divulging to any person or entity the contents of a communication. It also prohibits covered entities from knowingly divulging to any governmental entity customer records or other information. See Stored Communications Act of 1986, 18 U.S.C. § 2702(a) (2020).

13 There is no definition of "record" in the SCA, but courts have interpreted the term to include some data revealing a customer's location, most notably cell-site location data. For example, in *Carpenter v. United States*, the U.S. Supreme Court addressed the application of § 2703 of the SCA to cell phone location data. The Court held that a warrant was required to obtain seven days of historical cell-site location information (CSLI) obtained from a suspect's wireless carrier, pursuant to an order issued by a federal magistrate judge under the act. *Carpenter,* 138 S. Ct. at 2213. Location or proximity data may also be considered the "content" of a communication, especially if the purpose of a service is to record or communicate such data. For example, Google has argued that its location history feature acts as a journal logging a person's whereabouts, with the retained data therefore being the "content" of an entry. Brief of Amicus Curiae Google LLC in Support of Neither Party Concerning Defendant's Motion to Suppress Evidence from a "Geofence" General Warrant (ECF No. 29), United States v. Chatrie, No. 3:19-CR-00130 (E.D. Va.), https://www.nacdl.org/getattachment/723adf0b-90b1-4254-ab82-e5693c48e951/191220-chatrie-google-amicus-brief.pdf.

14 The Telecommunications Act prohibits covered entities from disclosing customer proprietary network information (CPNI) to any entity, including the government, unless an exception applies. See Communications Act of 1934, 47 U.S.C. § 222(c)(1) (2020) ("Except as required by law or with the approval of the customer, a telecommunications carrier that receives or obtains customer proprietary network information by virtue of its provision of a telecommunications service shall only use, disclose, or permit access to individually identifiable customer proprietary network information in its provision of (A) the telecommunications service from which such information is derived, or (B) services necessary to, or used in, the provision of such telecommunications service, including the publishing of directories."). Express prior authorization is required for a customer to approve the disclosure of their call location information. 47 U.S.C. § 222(f)(1). See also "FCC Proposes Over $200M in Fines for Wireless Location Data Violations," Federal Communications Commission, February 28, 2020, https://www.fcc.gov/document/fcc-proposes-over-200m-fines-wireless-location-data-violations. In the course of bringing this enforcement action, the FCC interpreted CPNI — without binding precedential effect — to broadly encompass "location information collected by carriers from a mobile device during a telephone call and . . . when the device is turned on and available for calls but not engaged in transmitting a voice conversation." In the Matter of AT&T, Inc., Notice of Apparent Liability for Forfeiture and Admonishment, 35 FCC Rcd. 1743, 2020 WL 1024412, at *11 (F.C.C. Feb. 28, 2020), https://docs.fcc.gov/public/attachments/FCC-20-26A1.pdf. However, as confirmed in a 2013 FCC declaratory ruling, the clearly established scope of location data protected as CPNI is limited to location information logged in connection with the *use* of a "telecommunication service" that is, when making or receiving a call. See "CPNI (Customer Proprietary Network Information)," Electronic Privacy Information Center, accessed May 5, 2020, https://epic.org/privacy/cpni (citing 2013 ruling). A 2016 FCC order would have expanded the definition of CPNI in a manner confirmed to cover location information intermittently logged in the course of a phone's connection to the network, but this order was repealed in 2017. "CPNI," Electronic Privacy Information Center.

15 In *Carpenter v. United States*, the U.S. Supreme Court addressed the application of Section 2703 of the SCA to cell phone location data. The Court held that a warrant was required to obtain seven days of historical CSLI from a suspect's wireless carrier. *Carpenter*, 138 S. Ct. at 2206.

16 See, e.g., Alan Z. Rozenshtein, "Disease Surveillance and the Fourth Amendment," *Lawfare*, April 7, 2020, https://www.lawfareblog.com/disease-surveillance-and-fourth-amendment.

17 This primer focuses generally on the federal statutory framework pertaining to the voluntary disclosure of cell phone location data to the government by entities that collect or maintain it. It does not, however, cover specific privacy protections available to children through the Children's Online Privacy Protection Act (COPPA). Children's Online Privacy Protection Act of 1998, 15 U.S.C. 6501–6505 (2020). Neither does this primer discuss state law. Some states might have more rigorous data protections. For example, California's Consumer Privacy Act (CCPA) provides consumers with the "right to know" information that businesses have collected or sold about them, a "right to opt out" of the sale of their personal information, and the right, in certain cases, to request that a business delete information collected about them. California Consumer Privacy Act, Cal. Civ. Code §§ 1798.105, 1798.100-1798.120 (2020). Geolocation data is included as a category of personal information subject to the CCPA. Cal. Civ. Code § 1798.140(o)(1)(G). Enforcement of the CCPA by the California attorney general is scheduled to begin on July 1, 2020. A coalition of civil liberties and consumer groups have called on the California Attorney General to investigate Grindr, Tinder, and other smartphone apps and ad tech companies for CCPA violations for sharing location data. ACLU of California et al. to Attorney General Xavier Becerra, "Re: Norwegian Consumer Council's Report Demonstrates How the Adtech Industry Fails to Respect Consumers Rights and Preferences," January 14, 2020, https://www.citizen.org/wp-content/uploads/CA-AG-Out-of-Control-NCC-1.14.20.pdf.

18 Jacob Hoffman-Andrews and Andrew Crocker, "How to Protect Privacy When Aggregating Location Data to Fight COVID-19," Electronic Frontier Foundation, April 6, 2020, https://www.eff.org/deeplinks/2020/04/how-protect-privacy-when-aggregating-location-data-fight-covid-19.

19 See, e.g., "COVID-19 Forecasts," Centers for Disease Control and Prevention, updated May 6, 2020, https://www.cdc.gov/coronavirus/2019-ncov/covid-data/forecasting-us.html; David A. Drew et al., "Rapid Implementation of Mobile Technology for Real-Time Epidemiology of COVID-19," *Science*, May 6, 2020, https://science.sciencemag.org/content/early/2020/05/05/science.abc0473/tab-pdf; "Privacy-Preserving Contact Tracing," Apple, accessed May 7, 2020, https://www.apple.com/covid19/contacttracing; and Steve Hendrix and Ruth Eglash, "Israel Is Using Cellphone Surveillance to Warn Citizens: You May Already Be Infected," *Washington Post*, March 19, 2020, https://www.washingtonpost.com/world/middle_east/israel-is-using-cellphone-surveillance-to-warn-citizens-you-may-already-be-infected/2020/03/19/68267294-69e7-11ea-b199-3a9799c54512_story.html.

20 See, e.g., Courtney Linder, "This MIT App Tracks the Spread of Coronavirus While Protecting Your Privacy," *Popular Mechanics*, March 18, 2020, https://www.popularmechanics.com/technology/apps/a31742763/coronavirus-app-private-kit-safe-paths; "Care19," North Dakota Response, accessed May 4, 2020, https://ndresponse.gov/coronavirus-resources/care19; and "Healthy Together Beta App," accessed May 7, 2020, https://coronavirus.utah.gov/healthy-together-app.

21 MIT Media Lab, "Safe Paths: A Privacy-First Approach to Contact Tracing," Massachusetts Institute of Technology News, April 10, 2020, http://news.mit.edu/2020/safe-paths-privacy-first-approach-con-

tact-tracing-0410. See also "Private Kit: Safe Paths; Privacy-by-Design Covid19 Solutions Using GPS Bluetooth for Citizens and Public Health Officials," Safe Paths (Massachusetts Institute of Technology), accessed May 4, 2020, https://safepaths.mit.edu; and "Safe Paths," Sculpting Evolution (Massachusetts Institute of Technology Media Lab), accessed May 4, 2020, https://www.media.mit.edu/projects/safepaths/overview.

22 Removing directly identifying elements from a dataset of location information is not enough to ensure anonymization or adequately protect privacy. For example, even without traditional identifiers like a name or address, it is possible to deduce someone's home and workplace from their movements alone — especially when this information is combined with public records or other data. Effective anonymization requires ensuring that individuals cannot be identified by linking two records within a dataset or linking separate datasets. Companies can take affirmative steps to shield against this kind of abuse, for instance by adding statistical noise to a data set or otherwise distorting individual data points or trajectories. See Matt Drange, "'Blind to the Data': Behind the Effort to Anonymously Track COVID-19 Carriers," *Protocol*, April 10, 2020, https://www.protocol.com/tripleblind-encryption-location-data-coronavirus; *Enlisting Big Data in the Fight Against Coronavirus: Hearing Before the Committee on Commerce, Science, and Transportation,* 116th Cong. (2020) (statement of Michelle Richardson, Director, Privacy and Data Project, Center for Democracy and Technology); and Jennifer Valentino et al., "Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret," *New York Times*, December 10, 2018, https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html.

23 Paresh Dave, "Three U.S. Local Governments to Adopt Coronavirus Contact Tracing App: MIT," Reuters, April 9, 2020, https://www.reuters.com/article/us-health-coronavirus-app/three-us-local-governments-to-adopt-coronavirus-contact-tracing-app-mit-idUSKCN21R3PR.

24 Ben Winslow, "Utah Launches App for COVID-19 Tracing," Fox 13, April 22, 2020, https://www.fox13now.com/news/local-news/utah-launches-app-for-covid-19-tracing; and "Care19," North Dakota Response.

25 "Apple and Google Partner on COVID-19 Contact Tracing Technology," *Keyword* (blog), Google, April 10, 2020, https://blog.google/inside-google/company-announcements/apple-and-google-partner-covid-19-contact-tracing-technology.

26 "Privacy-Safe Contact Tracing Using Bluetooth Low Energy," *Keyword* (blog), Google, accessed May 4, 2020, https://www.blog.google/documents/57/Overview_of_COVID-19_Contact_Tracing_Using_BLE.pdf.

27 "Care19," North Dakota Response.

28 The two main smartphone operating systems, iOS and Android (by Apple and Google, respectively), impose baseline restrictions on how third-party applications can leverage the capacities of the devices they are installed on. As most relevant here, neither system allows applications running in the background to freely send Bluetooth signals, limiting developers' ability to create proximity-based tracing applications that rely on that technology to continuously scan for potential contacts if they do not conform with the companies' own design requirements, as reflected in their joint contact tracing application programming interface (API). In this case, that contact matching must be done locally on individual devices, as opposed to centrally by the application's administrator. James Vincent, "Without Apple and Google, the UK's Contact-Tracing App Is in Trouble," *Verge,* May 5, 2020, https://www.theverge.com/2020/5/5/21248288/uk-covid-19-contact-tracing-app-bluetooth-restrictions-apple-google. See also Josh Taylor, "Covidsafe App is Not Working Properly on iPhones, Authorities Admit," *Guardian*, May 6, 2020, https://www.theguardian.com/world/2020/may/06/covidsafe-app-is-not-working-properly-on-iphones-authorities-admit; Dan Grummett, "Alberta Contact Tracing App Can't Run in the Background on iPhones," CTV News, May 5, 2020, https://edmonton.ctvnews.ca/alberta-contact-tracing-app-can-t-run-in-the-background-on-iphones-1.4926476; and Aradhana Aravindan and Sankalp Phartiyal, "Bluetooth Phone Apps for Tracking COVID-19 Show Modest Early Results," Reuters, April 21, 2020, https://www.reuters.com/article/us-health-coronavirus-apps/bluetooth-phone-apps-for-tracking-covid-19-show-modest-early-results-idUSKCN2232A0 ("A big complaint about [Singapore's] TraceTogether [which relies on centralized matching based on Bluetooth proximity logs] is that it doesn't work in the 'background' on an iPhone, meaning the app has to be open at all times, which drains power and can interfere with other processes. Apple does not permit iPhone apps running in the background to access Bluetooth, for security reasons.").

29 Vi Hart et al., *Outpacing the Virus: Digital Response to Containing the Spread of COVID-19 While Mitigating Privacy Risks*, Edmond J. Safra Center for Ethics, April 3, 2020, 17, https://ethics.harvard.edu/files/center-for-ethics/files/white_paper_5_outpacing_the_virus_final.pdf; Leo Kelion, "NHS Rejects Apple-Google Coronavirus App Plan," BBC News, April 27, 2020, https://www.bbc.com/news/technology-52441428; and Alex Hern, "Digital Contact Tracing Will Fail Unless Privacy Is Respected, Experts Warn," *Guardian*, April 20, 2020, https://www.theguardian.com/world/2020/apr/20/coronavirus-digital-contact-tracing-will-fail-unless-privacy-is-respected-experts-warn.

30 "Care19," North Dakota Response.

31 Daniel Estrin, "Israel Begins Tracking and Texting Those Possibly Exposed to the Coronavirus," NPR, March 19, 2020, https://www.npr.org/2020/03/19/818327945/israel-begins-tracking-and-texting-those-possibly-exposed-to-the-coronavirus; Gwen Ackerman and Yaacov Benmeleh, "Israeli Spyware Firm Wants to Track Data to Stop Coronavirus Spreading," Bloomberg, March 17, 2020, https://www.bloomberg.com/news/articles/2020-03-17/surveillance-company-nso-supplying-data-analysis-to-stop-virus; Noa Landau, "In Dead of Night, Israel Approves Harsher Coronavirus Tracking Methods Than Gov't Stated," *Haaretz*, March 17, 2020, https://www.haaretz.com/israel-news/.premium-cellphone-tracking-authorized-by-israel-to-be-used-for-enforcing-quarantine-orders-1.8681979; and David M. Halbfinger et al., "To Track Coronavirus, Israel Moves to Tap Secret Trove of Cellphone Data," *New York Times*, March 16, 2020, https://www.nytimes.com/2020/03/16/world/middleeast/israel-coronavirus-cellphone-tracking.html

32 Ackerman and Benmeleh, "Israeli Spyware Firm Wants to Track Data"; Halbfinger et al., "To Track Coronavirus, Israel Moves to Tap Secret Trove"; Landau, "In Dead of Night, Israel Approves Harsher Coronavirus Tracking Methods"; and Estrin, "Israel Begins Tracking and Texting Those Possibly Exposed."

33 "Israel's Top Court Says Government Must Legislate COVID-19 Phone-Tracking," Reuters, April 26, 2020, https://www.nytimes.com/reuters/2020/04/26/technology/26reuters-health-coronavirus-israel-monitoring.html.

34 Max S. Kim, "Seoul's Radical Experiment in Digital Contact Tracing," *New Yorker*, April 17, 2020, https://www.newyorker.com/news/news-desk/seouls-radical-experiment-in-digital-contact-tracing. Other efforts in South Korea involve requiring people coming into the country to record their symptoms on an app that also tracks location. See Josh Smith et al., "Ahead of the Curve: South Korea's Evolving Strategy to Prevent a Coronavirus Resurgence," Reuters, April 15, 2020, https://www.reuters.com/article/us-health-coronavirus-southkorea-respons/ahead-of-the-curve-south-koreas-evolving-strategy-to-prevent-a-coronavirus-resurgence-idUSKCN21X0MO.

35 Isobel Asher Hamilton, "South Korea Gives Out Detailed Information About Patients' Whereabouts," *Business Insider*, April 14, 2020, https://www.businessinsider.com/countries-tracking-citizens-phones-coronavirus-2020-3#south-korea-gives-out-detailed-information-about-patients-whereabouts-2.

36 "Coronavirus Privacy: Are South Korea's Alerts Too Revealing?," BBC News, March 5, 2020, https://www.bbc.com/news/world-asia-51733145.

37 Byron Tau, "Government Tracking How People Move Around in

Coronavirus Pandemic," *Wall Street Journal*, March 28, 2020, https://www.wsj.com/articles/government-tracking-how-people-move-around-in-coronavirus-pandemic-11585393202.

38 Tony Romm et al., "U.S. Government, Tech Industry Discussing Ways to Use Smartphone Location Data to Combat Coronavirus," *Washington Post*, March 17, 2020, https://www.washingtonpost.com/technology/2020/03/17/white-house-location-data-coronavirus.

39 Jen Fitzpatrick and Karen DeSalvo, "Helping Public Health Officials Combat COVID-19," *Keyword* (blog), Google, April 3, 2020, https://www.blog.google/technology/health/covid-19-community-mobility-reports.

40 "Apple Makes Mobility Data Available to Aid COVID-19 Efforts," Apple Newsroom, April 14, 2020, https://www.apple.com/newsroom/2020/04/apple-makes-mobility-data-available-to-aid-covid-19-efforts.

41 This analysis is narrowly focused. It does not evaluate possible governmental attempts to compel disclosure by relying on an emergency power or another legal authority that supersedes these statutes. It also does not consider constitutional issues implicated by these policies, only statutory questions.

42 See COVID-19 Consumer Data Protection Act of 2020, S. 3663, 116th Cong. (2020); and The Public Health Emergency Privacy Act, S. 3749, 116th Cong. (2020).

43 Both the Telecommunications Act and the SCA have consent exceptions, which are described in further detail in the following paragraphs.

44 To the extent these applications rely on a device's own Bluetooth and GPS methods to derive location, rather than cell-site data obtained from a wireless carrier, the Telecommunications Act would likely not be relevant.

45 The SCA applies to both "contents" and "records." There is no definition of "record" in the SCA, but the term is generally understood to encompass "envelope" or ancillary information, meaning information relating to when and how a message is communicated. The meaning or substance of the message itself is better characterized as "content." Orin S. Kerr, "A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It," *George Washington Law Review* 72 (2004): 1228. Courts have interpreted the term "record" to include some data revealing a customer's location, most notably cell-site location data. See, e.g., *Carpenter*, 138 S. Ct. at 2206 (noting the SCA permits the government to compel the disclosure of certain telecommunications records and finding that a warrant is required when the government seeks seven days of cell-site location information pursuant to the statute). Where the sole purpose of a particular application is to collect location or proximity information, such data might be less like "envelope" information and more akin to the contents of a communication. So long as location or proximity data is characterized as either a record or content, it is covered by the SCA. There are, however, greater protections for the contents of a communication: Section 2702(a) of the SCA prohibits providers of electronic communication services and remote computing services from knowingly divulging to *any person or entity* the contents of a communication (not just the government, as with a record). 18 U.S.C. § 2702(a).

46 The SCA applies to providers of electronic communication services (ECS), such as phone and messaging services, and remote computing service (RCS), which are data storage and processing services. See 18 U.S.C. §§ 2702(a)(3), 2510(15), 2711(2). The SCA was passed as part of the Electronic Communications Privacy Act in the 1980s, and the distinction between ECS and RCS is mostly outdated. Today, a provider like Gmail generally does both types of functions. See Kerr, "A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It," 1214–1215. As mentioned previously, the prohibition in the SCA on sharing consumer records with government entities applies equally to RCS and ECS. See 18 U.S.C. § 2702(a)(3).

47 Google, "Exposure Notification — Frequently Asked Questions," May 2020, https://covid19-static.cdn-apple.com/applications/covid19/current/static/contact-tracing/pdf/ExposureNotification-FAQv1.0.pdf ("Only public health authorities will have access to this technology and their apps must meet specific criteria around privacy, security, and data control.").

48 47 U.S.C. § 222(h)(2).

49 See, e.g., Brian Fung, "Uber Settles with FTC over 'God View' and Some Other Privacy Issues," *Los Angeles Times*, August 15, 2017, https://www.latimes.com/business/technology/la-fi-tn-uber-ftc-20170815-story.html; and Edith Ramirez et al., *Data Brokers: A Call for Transparency and Accountability, Federal Trade Commission*, May 2014, https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

50 Section 5 of the Federal Trade Commission Act gives the FTC broad jurisdiction to regulate "persons, partnerships, or corporations" to prevent them "from using unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce." Federal Trade Commission Act of 1914, 15 U.S.C. § 45(a)(2) (2020). However, there are several exceptions to this broad mandate. The exception most applicable to this primer is for "common carriers," which has been interpreted very narrowly. It is generally recognized that the FTC can regulate any activity of common carriers like AT&T and T-Mobile apart from their provision of communication services. This includes regulating their data privacy actions and policies. See Fed. Trade Comm'n v. AT&T Mobility LLC, 883 F.3d 848, 863 (9th Cir. 2018) ("We conclude that the exemption in Section 5 of the FTC Act — "except . . . common carriers subject to the Acts to regulate commerce" — bars the FTC from regulating "common carriers" only to the extent that they engage in common-carriage activity. By extension, this interpretation means that the FTC may regulate common carriers' non-common-carriage activities."); *FCC-FTC Consumer Prot. Memorandum of Understanding*, 2015 WL 7261839, at *1 (OHMSV Nov. 16, 2015) ("The agencies express their belief that the scope of the common carrier exemption in the FTC Act does not preclude the FTC from addressing non-common carrier activities engaged in by common carriers.").

51 15 U.S.C. § 45(a)(2) ("The Commission is hereby empowered and directed to prevent persons, partnerships, or corporations . . . from using unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce.").

52 "FTC Testifies on Geolocation Privacy," Federal Trade Commission, June 4, 2014, https://www.ftc.gov/news-events/press-releases/2014/06/ftc-testifies-geolocation-privacy.

53 Rob Copeland, "Google Offers User Location Data to Health Officials Tackling Coronavirus," *Wall Street Journal*, April 3, 2020, https://www.wsj.com/articles/google-offers-user-location-data-to-health-officials-tackling-coronavirus-11585893602; and Romm et al., "U.S. Government, Tech Industry Discussing Ways to Use Smartphone Location Data to Combat Coronavirus."

54 "Google and YouTube Will Pay Record $170 Million for Alleged Violations of Children's Privacy Law," Federal Trade Commission, September 4, 2019, https://www.ftc.gov/news-events/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations; "FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook," Federal Trade Commission, July 24, 2019, https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions (alleged violation of 2012 order).

55 "FTC Imposes $5 Billion Penalty."

56 "Privacy Policy," Apple, updated December 21, 2019, https://www.apple.com/legal/privacy/en-ww ("We also collect data in a form that does not, on its own, permit direct association with any specific individual. We may collect, use, transfer, and disclose non-personal information for any purpose. . . . Aggregated data is considered non-personal information for the purposes of this Privacy Policy."); "Privacy & Terms," Google, March 31, 2020, https://policies.google.com/privacy?hl=en-US ("We may share non-personally identifiable

information [that is recorded about users so that it no longer reflects or references an individually-identifiable user] publicly and with our partners."); "Twitter Privacy Policy," Twitter, January 1, 2020, https://cdn.cms-twdigitalassets.com/content/dam/legal-twitter/site-assets/privacy-page-gdpr/pdfs/Twitter-Privacy-Policy-EN.pdf ("We share or disclose non-personal data, such as aggregated information like the total number of times people engaged with a Tweet, demographics, the number of people who clicked on a particular link or voted on a poll in a Tweet (even if only one did), the topics that people are Tweeting about in a particular location, some inferred interests, or reports to advertisers about how many people saw or clicked on their ads."); "Data Policy," Facebook, updated April 19, 2018, https://www.facebook.com/full_data_use_policy ("We provide aggregated statistics and insights that help people and businesses understand how people are engaging with their posts, listings, Pages, videos and other content on and off the Facebook Products. . . . We share information about you with companies that aggregate it to provide analytics and measurement reports to our partners.").

57 See n. 46.

58 Department of Justice, *Sharing Cyberthreat Information under 18 USC § 2702(A)(3)*, May 2014, https://info.publicintelligence.net/DoJ-SharingCyberthreats.pdf.

59 See n. 46.

60 See n. 14.

61 Examples of electronic communication services (ECS) covered by the SCA include providers of messaging or social media services like Facebook or Twitter. See, e.g., Facebook, Inc. v. Superior Court, 417 P.3d 725, 740 (Cal. 2018) ("Prior decisions have found that Facebook and Twitter qualify as either an ECS or RCS provider and hence are governed by section 2702 of the SCA. . . . We see no reason to question this threshold determination."); Ehling v. Monmouth-Ocean Hosp. Serv. Corp., 961 F. Supp. 2d 659, 667 (D.N.J. 2013) ("Facebook provides its users with the ability to send and receive electronic communications, including private messages and Facebook wall posts. Accordingly, Facebook is an electronic communication service provider."); and Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 980 (C.D. Cal. 2010) (holding that because Facebook, MySpace, and Media Temple provide private messaging, email, or electronic bulletin board services, they constitute ECS within the meaning of the SCA).

62 Examples of remote computing services (RCS) covered by the SCA include companies that permit users to upload content, such as YouTube, as well as social media companies that store historical posts, such as Facebook. See *Crispin*, 717 F. Supp. 2d at 980 (finding social networking sites function as remote communication service (RCS) providers with respect to "wall" postings and comments posted on an account holder's web page); compare Viacom Int'l Inc. v. YouTube Inc., 253 F.R.D. 256, 264 (S.D.N.Y. 2008) (determining that YouTube acted as a provider of RCS in regard to user-uploaded videos that had been designated private via YouTube's privacy settings) with Yunker v. Pandora Media, Inc., No. 11-CV-03113, 2013 WL 1282980, at *9 (N.D. Cal. Mar. 26, 2013) (holding Pandora is not a RCS and distinguishing *Viacom* because in that case "it was clear that users of YouTube.com could upload videos to the website, which then stored those videos. . . . In contrast, Yunker does not allege that users of Pandora's service can upload and store music on Pandora.").

63 Google has argued that its Location History feature acts as a journal logging a person's whereabouts, with the retained data therefore being the "content" of an entry. Brief of Amicus Curiae Google LLC, United States v. Chatrie.

64 Data stored locally on cell phones falls outside the scope of the SCA. As one court explained, these devices do not "provide an electronic communication service simply by virtue of enabling use of electronic communication services." See In re iPhone Application Litig., 844 F. Supp. 2d 1040, 1058 (N.D. Cal. 2012). However, cloud storage services are considered RCS. See Orin Kerr, "The Next Generation Communications Privacy Act," *University of Pennsylvania Law Review* 162 (2014); and Jeffrey Paul DeSousa, "Self-Storage Units and Cloud Computing: Conceptual and Practical Problems with the Stored Communications Act and Its Bar on ISP Disclosures to Private Litigants," *Georgetown Law Journal* 102 (2013). Similarly, messaging services like iMessage would seem to fall under ECS following Crispin, 717 F. Supp. 2d at 981–82 (finding Facebook's and Myspace's private messaging functions are ECS).

65 The SCA prohibits ECS and RCS providers from disclosing the "contents" of a communication to any entity but only prohibits the disclosure of "records" to government entities. Thus, ECS and RCS providers can disclose "records" to third parties like data brokers. However, some scholars have argued that if it is known this information will be shared with the government by the data broker, the covered entity might be liable under SCA. Gilad Edelman, "Can the Government Buy Its Way around the Fourth Amendment?," *Wired*, February 11, 2020, https://www.wired.com/story/can-government-buy-way-around-fourth-amendment.

66 "FCC Proposes Over $200M in Fines for Wireless Location Data Violations."

67 Edelman, "Can the Government Buy Its Way around the Fourth Amendment?" ("Nathan Freed Wessler, the ACLU lawyer who successfully argued Carpenter's case at the Supreme Court, said there are at least two ways in which this arrangement [of the government buying location data from third parties] could violate the law. The first concerns the companies originally gathering location data, rather than the government. Under the Stored Communications Act of 1986, companies that store and transmit user data are generally prohibited from 'knowingly' sharing those records with the government. That, Wessler said, probably doesn't apply to a broker like Venntel that doesn't deal with consumers directly. But it could apply to the app makers who are passing data along to companies like Venntel, if they know it will eventually end up in the government's hands.").

68 47 U.S.C. § 222(f) ("without the express prior authorization of the customer, a customer shall not be considered to have approved the use or disclosure of or access to . . . call location information"). In 2007, the FCC modified its rules to require carriers to obtain opt-in consent from customers before disclosing CPNI data to a carrier's joint venture partners or independent contractors for the purposes of marketing. 47 C.F.R. § 64.2007 (2020). See In re Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information & Other Customer Information, 22 FCC Rcd 6927, https://docs.fcc.gov/public/attachments/FCC-07-22A1.pdf; and 18 U.S.C. §§ 2702(b)(3), (c)(3), 2703(c)(C).

69 See, e.g., Airbnb, Inc. v. City of New York, 373 F. Supp. 3d 467, 496–97 (S.D.N.Y. 2019); Rousset v. AT&T Inc., No. 14 Civ. 843, 2015 WL 9473821, at *8 (W.D. Tex. Dec. 28, 2015) (holding that plaintiff adopted Yahoo's terms of service and so consented to the monitoring of his communications and waived any privacy protections under the ECPA); In re Yahoo Mail Litig., 7 F.Supp.3d 1016, 1029 (N.D. Cal. 2014) (holding that Yahoo Mail users who accepted Yahoo's terms of service consented to the interception of their emails); and Viacom Int'l Inc., 253 F.R.D. at 264–65.

70 Rather, they tend to allow disclosure for compliance with legal orders, such as subpoenas or "enforceable governmental request[s]," or if the firm believes in good faith it needs to release the data to comply with the law. "Privacy Policy," Apple ("It may be necessary — by law, legal process, litigation, and/or requests from public and governmental authorities within or outside your country of residence — for Apple to disclose your personal information. We may also disclose information about you if we determine that for purposes of national security, law enforcement, or other issues of public importance, disclosure is necessary or appropriate."); "Privacy & Terms," Google ("We will share personal information outside of Google if we have a good-faith belief that access, use, preservation, or disclosure of the information is reasonably necessary to meet any applicable law, regulation, legal process, or enforceable governmental request."); "Let's Take a Look at the Full Verizon Privacy Policy," Verizon, accessed May 7, 2020, https://www.verizon.com/about/

privacy/full-privacy-policy#acc-item-35 ("We may disclose personally identifiable information to a governmental entity to comply with valid legal process"); "AT&T Privacy Policy," AT&T, March 16, 2020, https://about.att.com/csr/home/privacy/full_privacy_policy.html#how-share ("There are also times when we provide information that identifies you personally to other companies and entities, such as government agencies . . . without your explicit consent, but where authorized or required by law. Reasons to share include . . . complying with court orders, subpoenas, lawful discovery requests, and as otherwise authorized or required by law. Like all companies, we are required by law to provide information to government and law enforcement agencies . . . "); and "Data Policy," Facebook, ("We access, preserve and share your information with regulators, law enforcement or others . . . in response to a legal request (like a search warrant, court order or subpoena) if we have a good faith belief that the law requires us to do so. This may include responding to legal requests from jurisdictions outside of the United States when we have a good-faith belief that the response is required by law in that jurisdiction, affects users in that jurisdiction, and is consistent with internationally recognized standards.").

71 For example, studies have found many smartphone applications — including those that were commonly used — lacked basic privacy policies. "Location-Based Services Report," Federal Communications Commission, May 25, 2012, 20–21, https://www.fcc.gov/document/location-based-services-report.

72 See 18 U.S.C. § 2702(c)(4) ("A provider . . . may divulge a record or other information pertaining to a subscriber to or customer . . . to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of information relating to the emergency . . . "); and 18 U.S.C. § 2702(b)(8) ("A provider described in subsection (a) may divulge the contents of a communication — to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency . . . "). See also Alexander v. Verizon Wireless Servs., L.L.C., 875 F.3d 243 (5th Cir. 2017); People v. Moorer, 39 Misc. 3d 603, 959 N.Y.S.2d 868 (Co. Ct. 2013); United States v. Gilliam, No. 11 CRIM. 1083, 2012 WL 4044632 (S.D.N.Y. Sept. 12, 2012).

73 47 U.S.C. § 222; see also "CPNI," Electronic Privacy Information Center.

74 See, e.g., Jenna McLaughlin, "Coronavirus Pandemic Sparks New Calls for Personal Surveillance, and Concerns," *Yahoo News*, March 31, 2020, https://money.yahoo.com/coronavirus-pandemic-sparks-new-calls-for-personal-surveillance-and-concerns-204847804.html ("Al Gidari, the consulting director of privacy at Stanford's Center for Internet and Society and a former top private attorney representing companies like Google, told Yahoo News that 'neither the Stored Communications Act nor the Communications Act permit the government to compel disclosure or location information in response to a public health emergency.'").

75 *Carpenter*, 138 S. Ct. at 2217; and "Cell-Site Location Information Resources," Electronic Frontier Foundation, accessed May 12, 2020, https://www.eff.org/criminaldefender/cell-site-location/resources.

76 Alexandra Witze, "GPS Is Doing More Than You Thought," *Scientific American*, October 30, 2019 https://www.scientificamerican.com/article/gps-is-doing-more-than-you-thought; and "What is a GPS? How Does It Work?," Library of Congress, accessed May 12, 2020, https://www.loc.gov/everyday-mysteries/item/what-is-gps-how-does-it-work.

77 Bennett Cyphers, "Behind the One-Way Mirror: A Deep Dive Into the Technology of Corporate Surveillance," Electronic Frontier Foundation, December 2, 2019, https://www.eff.org/wp/behind-the-one-way-mirror; and "How Does Bluetooth Work?," *Scientific American*, November 5, 2007, https://www.scientificamerican.com/article/experts-how-does-bluetooth-work/.

78 Dieter Holger, "How 'Free' Wi-Fi Hotspots Can Track Your Location Even When You Aren't Connected," *PCWorld*, November 1, 2018, https://www.pcworld.com/article/3315197/free-wi-fi-hotspots-can-track-your-location-even-when-you-arent-connected.html; and Cyphers, "Behind the One-Way Mirror."

79 The Stored Communications Act (SCA) prohibits covered entities from knowingly divulging to any person or entity the contents of a communication. It also prohibits covered entities from knowingly divulging to any governmental entity customer records or other information. See Stored Communications Act of 1986, 18 U.S.C. § 2702(a).

80 See n. 45.

81 Department of Justice, *Sharing Cyberthreat Information Under 18 USC § 2702(a)(3)*.

82 See n. 14.

83 The Telecommunications Act can be plausibly interpreted to cover de-identified data. However, the FCC has not yet formally confirmed that it does, and wireless carriers do not yet appear to conceive of its coverage that way. See In the Matter of the Petition of Public Knowledge et al., Petition for Declaratory Ruling that the Sale of Non-Aggregate Call Records by Telecommunications Providers Without Customers' Consent Violates Section 222 of the Communications Act, WC Docket No. 13-306 (F.C.C. December 11, 2013), https://www.publicknowledge.org/files/2013-12-11-Final-CPNI-Petition-Signed.pdf (the Telecommunications Act covered de-identified customer data). A 2016 FCC rule that was repealed in 2017 under the Congressional Review Act incorporated a broader definition of protected information so as to limit the disclosure of formally de-identified data. Federal Communications Commission, "Protecting the Privacy of Customers of Broadband and Other Telecommunications Services," *Federal Register* 81, no. 232 (December 2, 2016), https://www.govinfo.gov/content/pkg/FR-2016-12-02/pdf/2016-28006.pdf.

84 Recent examples of the FTC's data privacy enforcement actions include *United States of America v. Facebook, Inc.*, where Facebook agreed to pay a $5 billion penalty and to implement new privacy measures after the FTC found the company had violated a previous agreement with the FTC regarding disclosure of customers' data with third-party applications. United States of America v. Facebook, Inc., No. 19-cv-2184 (D.D.C. filed July 24, 2019), https://www.ftc.gov/system/files/documents/cases/182_3109_facebook_order_filed_7-24-19.pdf. Similarly, with *In the Matter of Cambridge Analytica*, the FTC alleged Cambridge Analytica used deceptive tactics to collect personal information from tens of millions of Facebook users for voter profiling and targeting. In the Matter of Cambridge Analytica, No. 9383 (filed Dec. 6, 2019), https://www.ftc.gov/system/files/documents/cases/d09389_comm_final_opinionpublic.pdf.

85 "FTC Testifies on Geolocation Privacy," Federal Trade Commission.

86 One Senate proposal to "protect the privacy of consumers' . . . proximity data, and geolocation data during the coronavirus public health crisis" would legislatively designate such disclosure as an unfair or deceptive act or practice under the FTC Act. COVID-19 Consumer Data Protection Act of 2020, S. 3663.

87 45 C.F.R. §§ 160 and 164; and Office for Civil Rights, U.S. Department of Health and Human Services, Summary of HIPAA Privacy Rule, May 2003, https://www.hhs.gov/sites/default/files/privacysummary.pdf.

88 National Institutes of Health, U.S. Department of Health and Human Services, "How Can Covered Entities Use and Disclose Protected Health Information for Research and Comply with the Privacy Rule?," accessed May 12, 2020, https://privacyruleandresearch.nih.gov/pr_08.asp.

89 See n. 46.

90 Telephone companies are generally considered to be providers of ECS. See S. Rep. No. 99-541, at 14, reprinted in 1986 U.S.C.C.A.N. 3555, 3568, https://www.justice.gov/sites/default/files/jmd/

legacy/2014/08/10/senaterept-99-541-1986.pdf ("Existing telephone companies and electronic mail companies are providers of electronic communication services.").

91 See n. 61.

92 See n. 62.

93 Generally, cloud storage services like iCloud are considered RCS. See Jeffrey Paul DeSousa, "Self-Storage Units and Cloud Computing: Conceptual and Practical Problems with the Stored Communications Act and Its Bar on ISP Disclosures to Private Litigants," Georgetown Law Journal 102 (2013); and Kerr, "The Next Generation Communications Privacy Act." Similarly, messaging services like iMessage would seem to fall under ECS following Crispin, 717 F. Supp. 2d at 981–82 (finding Facebook's and Myspace's private messaging functions are ECS). However, personal computers and cell phones fall outside the scope of the SCA. As one court explained, these devices do not "provide an electronic communication service simply by virtue of enabling use of electronic communication services." See In re iPhone Application Litig., 844 F. Supp. 2d at 1058. Similarly, courts have found that emails stored on a personal computer are not stored communications subject to the SCA. Pure Power Boot Camp v. Warrior Fitness Boot Camp, 587 F. Supp. 2d 548, 555 (S.D.N.Y. 2008).

94 As one court explained, operators of commercial websites like Amazon or JetBlue that have email capabilities to communicate with their customers generally do not fall within the ambit of the ECS or RCS providers for purposes of the SCA. Combier v. Portelos, No. 17-CV-2239, 2018 WL 4678577, at *3 (E.D.N.Y. Sept. 29, 2018), aff'd, 788 F. App'x 774 (2d Cir. 2019); see also Crowley v. CyberSource Corp., 166 F. Supp. 2d 1263, 1270 (N.D. Cal. 2001) (finding Amazon, as a retailer, did not provide ECS or RCS when it used email to communicate with customers).

95 Section 222 of the Telecommunications Act applies to telecommunications carriers. Examples of telecommunications carriers include major wireless providers like Verizon, AT&T, and T-Mobile. The term is defined by statute as "any provider of telecommunications services." See 47 U.S.C. § 153(51).

96 See n. 50.

97 See Ramirez et al., *Data Brokers: A Call For Transparency and Accountability*.

98 See n. 50.

99 The FTC does not have jurisdiction over most nonprofit organizations because the FTC Act defines "corporation" as an entity "organized to carry on business for its own profit or that of its members." 15 U.S.C. § 44.

100 45 C.F.R. § 160.103.

101 18 U.S.C. § 2702(a)(3).

102 See n. 15.

103 Brief of Amicus Curiae Google LLC , United States v. Chatrie.

104 The term "customer proprietary network information" is defined as "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship." 47 U.S.C. § 222(h)(1). Express prior authorization is required for a customer to approve the disclosure of their call location information. 47 U.S.C. § 222(f)(1).

105 15 U.S.C. § 45(a)(1).

106 For example, in a 2011 enforcement action, the FTC alleged that Facebook had violated the FTC Act and deceived consumers by telling them they could keep their information on Facebook private and then repeatedly allowing it to be shared and made public. The resulting consent order settling the case prohibited Facebook from misrepresenting the privacy or security of "covered information," which included physical location information. In the Matter of Facebook, No. 092-3184 (D.D.C. 2011), https://www.ftc.gov/sites/default/files/documents/cases/2011/11/111129facebookagree.pdf.

107 45 C.F.R. § 160.103.

108 The emergency exception of the SCA requires that the disclosing provider believe in good faith that there is (1) an emergency involving danger of death or serious physical injury to any person, that it (2) requires disclosure without delay of information, and that (3) it relates to the emergency. See 18 U.S.C. §§ 2702(b)(8), (c)(4).

109 Department of Justice, *Sharing Cyberthreat Information Under 18 USC § 2702(a)(3).*

110 The emergency exception of the Telecommunications Act is multifaceted. Part of the exception permits covered entities to disclose CPNI to "providers of information or database management services solely for purposes of assisting in the delivery of emergency services in response to an emergency." See 47 U.S.C. § 222(d)(4)(c).

111 See 47 U.S.C. § 222(c)(3).

112 Treatment includes the coordination or management of health care and related services by one or more health care providers and others, consultation between providers, and the referral of patients for treatment. See 45 C.F.R. §§ 164.502(a)(1)(ii), 164.506(c), and the definition of "treatment" at § 164.501.

113 45 C.F.R. § 164.501.

114 45 C.F.R. §§ 164.501, 164.512(b)(1)(i); to persons at risk: 45 C.F.R. § 164.512(b)(1)(iv); to prevent or lessen threat: 45 C.F.R. § 164.512(j).

115 Office of the Secretary, U.S. Department of Health and Human Services, "Enforcement Discretion Under HIPAA To Allow Uses and Disclosures of Protected Health Information by Business Associates." Some groups, including the World Privacy Forum, have voiced concerns about the business associate HIPAA waiver, noting that "in general, disclosures of PHI for public health purposes are reasonable and beneficial," but that this waiver is too broad. The waiver seems to allow business associates to make determinations about public health activities on their own, without guidance from a public health authority. Additionally, it only requires a business associate to act in good faith, which could "mean no more than 'we thought it might help.'" "World Privacy Statement on HIPAA Waiver of April 2, 2020 and its Consequential Impacts on Privacy," World Privacy Forum, April 6, 2020, https://www.worldprivacyforum.org/2020/04/april-2-2020-wpf-statement-on-covid-19-and-changes-in-hipaa-practices.

BRENNAN CENTER FOR JUSTICE

Brennan Center for Justice at New York University School of Law
120 Broadway // 17th Floor // New York, NY 10271
www.brennancenter.org