A FOURTH AMENDMENT LOOPHOLE?: AN EXPLORATION OF PRIVACY AND PROTECTION THROUGH THE MUSLIM PRO CASE

Isabelle Canaan*

ABSTRACT

Smartphone and mobile applications cater to our individualized preferences by using information gleaned from our online activity. These efficient and hyper-connected devices are extensions of our physical bodies, accompanying us everywhere we go and generating location data that is highly profitable on the open market. Much of this data is commercial and is increasingly purchased by government actors through a loophole which allows them to circumvent Fourth Amendment protections.

This Article highlights this constitutional loophole by focusing on the Muslim Pro data purchasing scheme. Location data captured by and collected from Muslim Pro, an application which offers services tailored to a Muslim audience and devout religious practice, was eventually, through a series of purchases, bought by components of the U.S. military. The U.S. Special Operations Command has admitted to using this type of location data to help carry out their missions. The government skirts Fourth Amendment protections through their warrantless acquisition of data which, although purportedly individually anonymized, draws from an application specifically serving the Muslim community. This less transparent route to surveillance further marginalizes and targets the Muslim community and exposes a troubling expansion of the U.S. government into the lives of private citizens. Using Muslim Pro as an example, this Article argues that current Fourth Amendment jurisprudence does not sufficiently protect privacy, liberty, and property rights in an era of mass surveillance, constant connectivity, and mobile monitoring. Consequently, we must continue to rethink what constitutes a reasonable expectation of privacy in an increasingly digital age.

---

* J.D. Columbia Law School 2021. Many thanks to Matthew Waxman and Daniel Richman for their guidance and feedback, and to the editors of *HRLR Online* for their exceptional editorial work.

TABLE OF CONTENTS

INTRODUCTION

In recent years, the public has become aware that various government agencies are purchasing commercially available, anonymized location data without receiving a warrant or subpoena as the Fourth Amendment would otherwise require.[1] The Department of Homeland Security ("DHS"), Customs and Border Patrol ("CBP"), and Immigration and Customs Enforcement ("ICE"), among others, have all allegedly bought commercially available cell phone location records.[2] Alarmingly, these government agencies have refused to disclose the legal authority under which they are justifying these purchases. In an October 2020 letter, Senator Ron Wyden (D-OR) and five of his colleagues urged the Inspector General to investigate CBP's warrantless use of commercial databases, with a particular focus on the legal analysis, if any, the agency performed prior to the surveillance[3] In December 2020, the American Civil Liberties Union ("ACLU") brought action under the Freedom of Information Act ("FOIA") to force DHS to release records about its purchase of cell phone location data for immigration enforcement and other purposes.[4] Both of these responses to

---

1. *See generally* Andrea Vittorio & Allyson Versprile, *IRS Use of Cell Phone Location Data Hits 'Legal Gray Area*,' BL (Oct. 7, 2020), https://news.bloomberglaw.com/privacy-and-data-security/irs-use-of-cell-phone-location-data-falls-in-legal-gray-area [https://perma.cc/W35J-WTU4] (explaining that the Internal Revenue Service's use of cell phone location data faces legal uncertainty relating to privacy concerns); Adi Robertson, *Secret Service Bought Access to Cellphone Location Data*, VERGE (Aug. 17, 2020), https://www.theverge.com/2020/8/17/21371886/secret-service-usss-locate-x-babel-street-foia-contract-report [https://perma.cc/5Z7L-9U2P] (reporting that the U.S. Secret Service, Customs and Border Control, and Immigration and Customs Enforcement have all used a third-party service which can track phone users' locations); Byron Tau & Michelle Hackman, *Federal Agencies Use Cellphone Location Data for Immigration Enforcement*, WALL ST. J. (Feb. 7, 2020), https://www.wsj.com/articles/federal-agencies-use-cellphone-location-data-for-immigration-enforcement-11581078600 (on file with the *Columbia Human Rights Law Review*) ("The Trump administration has bought access to a commercial database that maps the movements of millions of cellphones in America and is using it for immigration and border enforcement.").

2. Tau & Hackman, *supra* note 1; Opinion, *Apps Are Selling Your Location Data. The U.S. Government Is Buying,* WASH. POST (Feb. 9, 2020), https://www.washingtonpost.com/opinions/apps-are-selling-your-location-data-the-us-government-is-buying/2020/02/09/9d09475e-49e2-11ea-b4d9-29cc419287eb_story.html [https://perma.cc/K37Q-TCVR].

3. *See* Letter from Sen. Ron Wyden, et al., to Hon. Joseph Cuffari, Inspector Gen., DHS (Oct. 23, 2020), https://www.wyden.senate.gov/imo/media/doc/102320%20Wyden%20Warren%20Brown%20Markey%20Schatz%20Letter%20RE%20CBP%20Phone%20Tracking.pdf [https://perma.cc/8FQE-4KEQ].

4. *See ACLU*, *CLEAR FOIA Request Concerning Purchase and Use of Cell Phone Location Data*, ACLU (Dec. 3, 2020), https://www.aclu.org/legal-document/aclu-clear-foia-request-concerning-purchase-and-use-cell-phone-location-data [https://perma.cc/

unauthorized government surveillance reflect the outrage over the agencies' potential evasion of Fourth Amendment protections for location information, as well as profound public concern about the ability of government agencies to use location data opaquely.

Recent reports also indicate a troubling expansion in the type of government actors acquiring commercial location data. Federal documents have revealed that location data collected by a series of widely used applications has been sold to military contractors and the U.S. military.[5] One of these applications is Muslim Pro, which provides users with daily prayer times, a *Qibla* locator, and an Islamic calendar, among other functions.[6] Muslim Pro has been downloaded over 98 million times and is used by Muslims in over 200 countries.[7]

The data-collection-and-sale scheme worked as follows: Muslim Pro sent users' private location data to a data broker company called X-Mode, which sold the information to contractors, and thus by extension, the U.S. military, which claims to use the information for counterterrorism purposes.[8] If this is the case, this would be the latest instance in a troubling

---

G89T-HJHS] ("All contracts, memoranda of understanding, letters of commitment, licenses, subscription agreements, and other agreements with vendors . . . .").

5. Joseph Cox, *How the U.S. Military Buys Location Data from Ordinary Apps*, VICE: MOTHERBOARD (Nov. 16, 2020) [hereinafter *How the U.S. Military Buys Location Data*], https://www.vice.com/en/article/jgqm5x/us-military-location-data-xmode-locate-x [https://perma.cc/EU8J-DHP4] (uncovering U.S. military purchases of data from X-Mode, which procures data from apps including Muslim Pro and Muslim Mingle (a dating app), confirming the widespread use of Locate X (software used to locate and track mobile devices, and the purchase of additional location data from another vendor called Venntel)); DEFENSE INTELLIGENCE AGENCY ("DIA"), U-21-0002/OCC-1, CLARIFICATION OF INFORMATION BRIEFED DURING DIA'S 1 DECEMBER BRIEFING ON CTD (Jan. 15, 2021) ("DIA currently provides funding to another agency that purchases commercially available geolocation metadata aggregated from smartphones.").

6. *MuslimPro's Features*, MUSLIMPRO, https://www.muslimpro.com/features [https://perma.cc/9TXK-9SXB]. *Qibla* is the direction towards the Kaaba, used as the direction of prayer for Muslims. As of January 28, 2021, it has been disclosed that data from at least five more similar Muslim prayer apps using X-Mode was sold in the same scheme. Joseph Cox, *More Muslim Apps Worked with X-Mode Which Sold Data to Military Contractors*, VICE (Jan. 28, 2021) [hereinafter *More Muslim Apps Worked with X-Mode*], https://www.vice.com/en/article/epdkze/muslim-apps-location-data-military-xmode [https://perma.cc/ZDU9-NAJ9].

7. *How the U.S. Military Buys Location Data*, *supra* note 5; Mobashra Tazamal, *MuslimPro's 'Data Sale' Benefiting the U.S. Army Is Betrayal that Puts Muslim Lives in Danger*, NEW ARAB (Nov. 24, 2020), https://english.alaraby.co.uk/opinion/muslimpros-data-sale-not-just-outrageous-betrayal [https://perma.cc/7AUQ-R4NE] (describing Muslim Pro, its widespread popularity, and its components).

8. *How the U.S. Military Buys Location Data*, *supra* note 5; Tazamal, *supra* note 7 ("Most apps are free but more often than not a user is most likely offering up personal data

series of revelations that various government agencies are circumventing Fourth Amendment "probable cause" warrant requirements by buying large tranches of anonymized location data from data brokers for unknown uses.[9]

These data-collection schemes raise the question of whether a warrant is required to protect the privacy of anonymized data purchased by an agency from a third party.[10] This question is further complicated when set against the history of government surveillance of Muslim American communities, the complicated counterterrorism and national security justifications, and the potential for intermingled collection of foreigners' data, legal under the Foreign Intelligence Surveillance Act ("FISA").[11]

This Article examines the quandaries posed by the commercial acquisition of anonymized location data by government entities. Part I provides a brief presentation of the relevant Fourth Amendment principles, with a focus on the reasonableness standard and the third-party doctrine. Part II uses this doctrinal background as a touchstone for the Muslim Pro case, paying special mind to the type of data being acquired and how the reasonable expectation of privacy has been interpreted. This Part also assesses why government agencies and the military are not using the expansive legal tools already at their disposal to forward their stated counterterrorism and national security purposes for data acquisition. Finally, Part III offers a series of next steps for both users and legislators outraged by the government's purchase of location data.

I. Fourth Amendment Overview

The Fourth Amendment structures the privacy relationship between an individual and the government, protecting "the right of people to

---

when using these services . . . .[and] [i]n the case of MuslimPro, one customer is the US military.").

9. In March 2020, investigative reporting revealed that U.S. Customs and Border Protection had purchased a software product called Locate X, which "allows investigators to draw a digital fence around an address or area, pinpoint mobile devices that were within the area, and see where else those devices have traveled." Federal records also revealed that the Secret Service and U.S. Immigration and Customs Enforcement have also used this technology. Charles Levinson, *Through Apps, Not Warrants, 'Locate X' Allows Federal Law Enforcement to Track Phones*, PROTOCOL (Mar. 5, 2020), https://www.protocol.com/government-buying-location-data [https://perma.cc/3UNU-YPB5]; *see* Gilad Edelman, *Can the Government Buy Its Way Around the Fourth Amendment?*, WIRED (Feb. 11, 2020), https://www.wired.com/story/can-government-buy-way-around-fourth-amendment/ [https://perma.cc/9URP-3FX3] ("[T]the Department of Homeland Security has been using commercially available cell phone location records for immigration and border enforcement.").

10. Vittorio & Versprile, *supra* note 1.

11. Tazamal, *supra* note 7; Foreign Intelligence Surveillance Act, 50 U.S.C. § 1881a.

be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." [12] A reasonable and constitutional Fourth Amendment search requires government officials to obtain a search warrant supported by probable cause.[13]

When evaluating a search's constitutionality, courts assess whether the individual whose person, house, paper, or effect is subject to the search had a reasonable expectation of privacy.[14] In his controlling concurrence in *Katz v. United States*, Justice Harlan set out the bi-dimensional test for an individual's reasonable expectation of privacy: "[F]irst that a person [has] exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[15] Yet, the Fourth Amendment does not establish "a general constitutional 'right to privacy.'" [16] For example, an individual does not enjoy a reasonable expectation of privacy or Fourth Amendment protection in "[w]hat a person knowingly exposes to the public, even in his own home or office."[17]

In *United States v. Miller* and *Smith v. Maryland*, the Supreme Court established the third-party doctrine, which states that an individual also does not enjoy a reasonable expectation of privacy when he or she shares information with a third party. In sharing this information, a person knowingly exposes private information and assumes the risk that it will be revealed.[18] Thus, the government can access that information without first acquiring a warrant.

Digital age innovations, including advancements in data collection by smartphones and applications, have challenged the third-party doctrine. Motivated by digital privacy concerns and recognizing the sheer amount of information disclosed to third parties daily, Congress passed the Electronic Communications Privacy Act ("ECPA") in 1986, which included the Stored

---

12. U.S. CONST., amend. IV.

13. *Id. See generally* Katz v. United States, 389 U.S. 347 (1967) (stating that searches conducted without prior approval pursuant to the Fourth Amendment are prohibited); Coolidge v. Hampshire, 403 U.S. 443 (1971) (finding that a neutral and detached judge must determine whether a probable cause exists); Illinois v. Gates, 462 U.S. 213, (1983) (holding that a totality of the circumstances test was required to establish probable cause); Groh v. Ramirez, 540 U.S. 551 (2004) (establishing that a constitutional warrant must include accurate information about what is to be searched).

14. *Id.*

15. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

16. *Id.* at 350.

17. *Id.* at 382.

18. Smith v. Maryland, 442 U.S. 735, 735–36 (1979); United States v. Miller, 425 U.S. 435, 442–43 (1976).

Communications Act ("SCA").[19] The SCA sets out rules for law enforcement when it acquires data from a third party, including when a warrant established by probable cause is necessary.[20]

Even with these increased statutory protections, the explosion in Global Positioning System ("GPS") and location tracking continued to challenge the efficacy of the pre-existing legal framework, necessitating a further evolution of the third-party doctrine. Unlike surveillance tactics of old, location data and GPS monitoring "generate[] a precise, comprehensive record of a person's public movements" that can be stored and utilized for years.[21] Since most smartphones constantly track and store location information, a person's movements can be easily pieced together.[22] As Chief Justice Roberts stated in *Riley v. California*, cell phones hold many of "the privacies of life."[23] The widespread and cheap availability of location data restructures the core Fourth Amendment relationship between an individual and the government in expansive, and potentially calamitous, ways.[24] More generally, the rapid transformation of daily life changed (and continues to change) the reasonable person's privacy expectation, requiring flexible and evolving privacy and reasonableness standards.[25] Acknowledging these changes, the Court, in *United States v. Jones* and *Riley v. California*, determined

---

19. Electronic Communications Privacy Act, 18 U.S.C. §§ 2510—23, 2701–12, 3121–27 (1986); Stored Communications Privacy Act, 18 U.S.C §§ 2701–12 (1986); Alan Z. Rozenshtein, *Fourth Amendment Reasonableness After Carpenter*, 128 YALE L.J. 943, 944 (2019).

20. Stored Communications Privacy Act, 18 U.S.C §§ 2701–12 (1986). Before *Carpenter*, the SCA required a government entity to acquire a warrant establishing probable cause before acquiring certain categories of content information. To access less sensitive information, like metadata, the government only needed a subpoena. For information that is more sensitive than metadata but less sensitive than privacy information, the government could only access the information if it "offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation." 18 U.S.C § 2703(d).

21. United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring).

22. Riley v. California, 573 U.S. 373, 396 (2014) ("Historic location information is a standard feature on many smart phones and can reconstruct someone's specific movements down to the minute.").

23. *Id.* at 403 (citation omitted); *see also id.* ("The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought.").

24. *Jones*, 565 U.S. at 416 (Sotomayor, J., concurring) ("[T]he government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse [and] [t]he net result is that GPS monitoring . . . may 'alter the relationship between citizen and government in a way that is inimical to democratic society.'") (quoting United States v. Cuevas–Perez, 640 F.3d 272, 285 (7th Cir. 2011) (Flaum, J., concurring)).

25. *Id.* at 427 (Alito, J., concurring).

that individuals have an expectation of privacy in their physical movements and that certain location-related surveillance incidents are excepted from the third-party doctrine.[26]

In *Carpenter v. United States*, the Court went one step further, determining how to interpret the third-party doctrine and the SCA in a digital world where personal location data is constantly generated and stored.[27] Here, the Federal Bureau of Investigation ("FBI") applied for court orders to obtain cell-side location information ("CSLI") for suspects, including Timothy Carpenter, for a string of robberies.[28] Under the relevant SCA provision, CSLI was not considered to be sensitive content-like data. Accordingly, the FBI did not have to demonstrate probable cause to obtain a warrant. Rather, the agency only had to "offer[] specific and articulable facts showing that there are reasonable grounds to believe" that the records sought were "relevant and material to an ongoing criminal investigation."[29] In a landmark ruling, the Supreme Court held that this "reasonable grounds" threshold was too low a standard to determine when to allow the government to access highly sensitive and revealing information like CSLI.[30] Today, if the government wants to acquire location data like CSLI from a third party, it must provide a warrant establishing probable cause.

The Court arrived at this decision for two reasons. First, it referenced its prior recognition "that individuals have a reasonable expectation of privacy in the whole of their physical movements."[31] CSLI, like GPS data, is "detailed, encyclopedic, and effortlessly compiled."[32] Even though CSLI data captures public movements, its revelatory and all-encompassing nature implicates the "privacies of life" protected by the

---

26. *Riley*, 573 U.S. at 373, 394–96, 403; *Jones*, 565 U.S. at 405–08 ("In *Katz v. United States*, we said that 'the Fourth Amendment protects people, not places' [and] . . . . [o]ur later cases have applied the analysis of Justice Harlan's concurrence in [*Katz*], which said that a violation occurs when government officers violate a person's 'reasonable expectation of privacy.'") (quoting Katz v. United States, 389 U.S. 3467, 351, 360 (1967)).

27. "The digital data at issue—personal location information maintained by a third party—does not fit neatly under existing precedents but lies at the intersection of two lines of cases. One set addresses a person's expectation of privacy in his physical location and movements. The other addresses a person's expectation of privacy in information voluntarily turned over to third parties." Carpenter v. United States, 138 S. Ct. 2206, 2209 (2018).

28. *Id.* at 2212.

29. *Id.* (citing the Stored Communications Act, 18 U.S.C. § 2703(d) (1994)).

30. *Id.* at 2221 ("[T]he Government must generally obtain a warrant supported by probable cause before acquiring such records [like cell-site location information].").

31. *Id.* at 2217.

32. *Id.* at 2216.

Fourth Amendment against arbitrary government invasions.[33] Second, regarding the third-party doctrine, the Court determined that, because of the indispensable nature of cell phones and the inability of the user to "avoid leaving behind a trail of location data," CSLI is not "shared" in a way that amounts to voluntary exposure.[34] The difference-in-degree of the type of data that is generated and collected has become a difference-in-kind for the Court, warranting a reevaluation of a person's reasonable privacy expectations and a heightened standard of government proof prior to access.

By favoring a flexible approach to the Fourth Amendment and the third-party doctrine, the Court has recognized the still-evolving privacy relationship between an individual and the government, and how that relationship is mediated and impacted by technological development.[35]

II. Muslim Pro, Reasonable Expectations of Privacy, and *Carpenter*

According to *Carpenter*, because of location data's depth, breadth, and comprehensive reach, the government must acquire a warrant establishing probable cause before accessing such data directly from third parties. However, in the Muslim Pro case, "the government is using its checkbook to try to get around *Carpenter*," by buying commercially available anonymized location data directly from data brokers.[36] In amassing a database of location data that, although purportedly individually anonymized, draws from an application specifically serving the Muslim community, the government is taking advantage of an even less transparent route to surveil a historically marginalized and targeted religious group.

Like the CSLI data in *Carpenter*, the Muslim Pro data is "personal location information maintained by a third party" and should be subject to

---

33. *Id.* at 2217 (citing Riley v. California, 573 U.S. 373, 452 (2014)). This understanding corresponds with the "mosaic theory" of privacy, which "is the idea that large scale or long-term collections of data reveal details about individuals in ways that are qualitatively different than single instances of observation and the related idea that as a consequence Fourth Amendment law should take account of that fact through a warrant requirement for 'big data' collection." Paul Rosenzweig, *In Defense of the Mosaic Theory*, LAWFARE (Nov. 29, 2017), https://www.lawfareblog.com/defense-mosaic-theory [https://perma.cc/9EPE-FZGP].

34. Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018).

35. "[T]he *Katz* test rests on the assumption that this hypothetical reasonable person has a well-developed and stable set of privacy expectations. But technology can change those expectations. Dramatic technological change may lead to periods in which . . . popular expectations are in flux and may ultimately produce significant changes in popular attitudes." United States v. Jones, 565 U.S. 400, 427 (2012) (Alito, J., concurring).

36. Levinson, *supra* note 9.

higher protection from arbitrary government intrusion.[37] If anything, technological innovation since *Carpenter*, coupled with the distinct characteristics of the Muslim Pro dataset, indicate that this data is even more comprehensive and deserving of increased protection from warrantless government collection.

Muslim Pro sent precise geolocation coordinates of users' phones and Wi-Fi network names to X-Mode through Software Development Kits ("SDKs").[38] Unlike cell-tower pings, which are external to the individual device itself, SDKs are bundles of code embedded directly into an application.[39] Data brokers like X-Mode develop this software and encourage application developers, with whom they work, to directly incorporate their SDK into an application.[40] The SDK collects the user's location data and sends it directly to X-Mode, who pays the application developers a fee based on the number of application users.[41] X-Mode is one of the largest data brokers of this type, with its SDKs currently present in around 400 applications, tracking 25 million devices inside the United States every month.[42] It sells the acquired location data to various clients, including defense contractors like the Sierra Nevada Corporation and Northrop Grumman, who work directly with the U.S. military.[43]

Constant monitoring is an essential component of the mosaic of privacy rationale that the Court has found requires protection. Location data collected through SDKs "generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations."[44] Additionally, the Court has already acknowledged that "'apps' offer a range of tools for managing detailed information about all aspects of a person's life."[45] While the data collected by Muslim Pro and sold to X-Mode is anonymized, the information is so precise that individuals are easily identifiable.[46] Moreover,

---

37. *Carpenter*, 138 S. Ct. at 2214.
38. *How the U.S. Military Buys Location Data*, *supra* note 5.
39. *Id.*
40. *Id.*
41. *Id.*
42. *Id.*; *'Untrue': Muslim Pro App Denies Selling User Data to U.S. Military*, AL JAZEERA (Nov. 18, 2020), https://www.aljazeera.com/news/2020/11/18/muslim-pro-app-denies-selling-user-data-to-us-military [https://perma.cc/P49Q-M2UZ] ("X-Mode . . . [also] said it tracks . . . 40 million [devices] elsewhere—including in the European Union, Latin America, and the Asia Pacific region.").
43. *How the U.S. Military Buys Location Data*, *supra* note 5.
44. United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor J., concurring).
45. Riley v. California, 573 U.S. 373, 396 (2014).
46. Aysha Khan, *MuslimPro, a Popular Prayer App, Stops Providing User Data to Firm Selling to U.S. Military*, RELIGION NEWS SERV. (Nov. 18, 2020), https://religion

the data at issue is collected from an application targeted at a particular religious community for a religious purpose. Thus, even if technically anonymized, the data inevitably reveals information about religious associations since Muslim Pro users are largely Muslim. Therefore, it meets, and surpasses, the type of revealing personal information – personal location data held by third parties - that concerned the Court in *Carpenter* and, thus, would require a warrant established by probable cause.

Users are also unaware that the applications they download come with SDKs that constantly transmit their precise location data to third parties. Like CSLI in *Carpenter*, these applications log locational data "without any affirmative act on the user's part beyond powering up."[47] Muslim Pro's application privacy policy did not make any reference to the possibility of sharing the user's data with X-Mode or other similar companies.[48] Muslim Pro users were never notified about the collection and transfer of data.[49] The scheme's revelation spurred outrage indicating that users did not expect that an application tailored to their spiritual needs would collect and sell location data to the same government agencies that

---

news.com/2020/11/18/muslim-prayer-times-app-stops-providing-user-data-to-firm-selling-to-us-military/ [https://perma.cc/L95Z-TPXD]; *'Untrue': Muslim Pro App Denies Selling User Data to U.S. Military*, *supra* note 42. As demonstrated by *New York Times* reporting and various academic studies, it is relatively cheap and easy to deanonymize this data. *See* Karl Bode, *Researchers Find 'Anonymized' Data Is Even Less Anonymous than We Thought*, VICE (Feb. 3, 2020), https://www.vice.com/en/article/dygy8k/researchers-find-anonymized-data-is-even-less-anonymous-than-we-thought [https://perma.cc/E8JA-ZERN] ("[A]nalysis from students at Harvard University shows that anonymization isn't the magic bullet companies like to pretend it is."); Stuart A. Thompson & Charlie Warzel, *Twelve Million Phones, One Dataset, Zero Privacy*, N.Y. TIMES (Dec. 19, 2019), https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html [https://perma.cc/PBK3-BTWN] ("[Although] the location data contains billions of data points with no identifiable information like names or email addresses . . . it's child's play to connect real names to the dots that appear on the maps."); Rocher et al., *Estimating the Success of Re-Identification in Incomplete Datasets Using Generative Models*, 10 NATURE COMMC'NS (2019), https://www.nature.com/articles/s41467-019-10933-3.pdf [https://perma.cc/6CH6-RABT] ("De-identification, the process of anonymizing datasets before sharing them, has been the main paradigm used in research and elsewhere to share data while preserving people's privacy . . . [y]et numerous supposedly anonymous datasets have recently been released and re-identified."); *How the U.S. Military Buys Location Data*, *supra* note 5 ("[In addition to the location data], [t]he data transfer [to X-Mode] also include[s] the name of the wifi network the phone was currently [connected] to, a timestamp, and information about the phone such as its model.").

47. Carpenter v. United States, 138 S. Ct. 2206, 2210 (2018).

48. Nadda Osman, *UK-Based Couple Threaten Legal Action over Muslim Pro Data Sharing*, MIDDLE EAST EYE (Nov. 27, 2020), https://www.middleeasteye.net/news/uk-muslim-pro-data-sharing-couple-legal-action [https://perma.cc/N7UV-6RT7].

49. *More Muslim Apps Worked with X-Mode*, *supra* note 6.

have surveilled them for years.[50] In response, the Islamic Leadership Council of New York urged members of its ninety organizations to delete the application.[51] Thus, absent any notification, the typical user does not reasonably expect, and is not voluntarily assuming the risk that their geolocation is being collected in bulk, much less sold by a data broker to a government contractor or the government.[52]

A. Potential Justifications for Warrantless Government Acquisition

For all the reasons stated above, government agencies and the military would need a *Carpenter* warrant establishing probable cause to acquire data like the Muslim Pro dataset. However, rather than going to court on a case-by-case basis, by purchasing location data from third parties, the government is exploiting a workaround.[53] When pressed by reporters, politicians, and the public to explain the legal justifications for the purchase of this information, DHS and CBP argue that *Carpenter* does not apply to location data purchased by the government.[54] Most recently, in a January 2021 memo, Defense Intelligence Agency ("DIA") analysts for Senator Ron Wyden's office stated that the "D.I.A. does not construe the *Carpenter* decision to require a judicial warrant endorsing purchase or use of commercially available data for intelligence purposes."[55]

It is impossible to know the extent of, or lack thereof, legal analysis conducted by government agencies to justify these purchases, because DHS and CBP have not responded directly to Senator Wyden's letter, or to FOIA

---

50. Tazamal, *supra* note 7. This reaction resonates with Justice Sotomayor's concurrence in *Jones*, which states, "I for one doubt that people would accept without complaint the warrantless disclosure to the government of a list of every Web site they had visited in the last week, or month, or year." United States v. Jones, 565 U.S. 400, 418 (2012) (Sotomayor J., concurring).

51. *See* Islamic Leadership Council of New York, FACEBOOK (Nov. 16, 2020), https://www.facebook.com/ShuraNewYork/photos/a.1910705805905416/2422084084767583/?type=3&theater (urging users to delete the application) (last visited Feb. 24, 2022).

52. Khan, *supra* note 46.

53. Tau & Hackman, *supra* note 1.

54. Letter from Sen. Ron Wyden, et al., to Hon. Joseph Cuffari, *supra* note 3, at 1; Dell Cameron, *Feds Find Fourth Amendment Workaround, Buy Phone Locations from Marketing Firms*, GIZMODO (Feb. 7, 2020), https://gizmodo.com/feds-find-fourth-amendment-workaround-buy-phone-locati-1841516436 [https://perma.cc/JD4M-S7F7].

55. Charlie Savage, *Intelligence Analysts Use U.S. Smartphone Location Data Without Warrants, Memo Says*, N.Y. TIMES (Jan. 25, 2021), https://www.nytimes.com/2021/01/22/us/politics/dia-surveillance-data.html [https://perma.cc/F48W-FBYP].

requests from the ACLU.[56] Moreover, in the Muslim Pro case, military and government agencies served with FOIA requests by the ACLU back in December 2020 have yet to respond.[57] Without full information on the extent of the scheme, there are a few grounds on which DHS, CBP, and the U.S. military could argue that their purchase of this location data is beyond *Carpenter*'s reach and legally permissible.

1. The Existing Statutory Vacuum

There are no current statutes that restrict acquisition of location data. The SCA, the most relevant federal statute on data privacy, only states that "certain kinds of communications can be produced by certain kinds of providers to the government with a warrant or a court order."[58] There are no statutes that restrict how commercial entities sell their data.[59] Therefore, while these purchases violate the spirit of *Carpenter* and its recognition that protecting data reasonably assumed private from government interference is essential, these purchases do not themselves amount to a per se violation of any federal statute.

2. National Security, Counterterrorism, and Intelligence

National security is one potential justification for extra-constitutional purchases of location data by government actors. According to federal records, location information was acquired through contractors purchasing from X-Mode for use in counterterrorism operations, and

---

56. *See* Letter from Sen. Ron Wyden, et al., to Hon. Joseph Cuffari, *supra* note 3; Complaint at 1, ACLU v. DHS, No. 1:20-cv-10083 (S.D.N.Y. Dec. 2, 2020), https://www.aclu.org/sites/default/files/field_document/1._complaint_1_0.pdf [https://perma.cc/65JP-WNAC] ("The agencies' purchases raise serious concerns that they are evading Fourth Amendment protections for cell phone location information by paying for access instead of obtaining a warrant . . . [and] more than nine months after the ACLU submitted its FOIA request . . . these agencies have produced no responsive records.").

57. *ACLU, CLEAR FOIA Request Concerning Purchase and Use of Cell Phone Location Data*, *supra* note 4.

58. *See* Stewart Baker, *The Cyberlaw Podcast: The Privacy and Europocrisy Oversight Board*, LAWFARE at 26:27 (Nov. 24, 2020), https://www.lawfareblog.com/cyberlaw-podcast-privacy-and-europocrisy-oversight-board [https://perma.cc/T4L6-Y9U2] ("In general, the U.S. statutes don't heavily regulate or restrict [market purchases of data that don't involve a surveillance device]. . . . FISA and the Wiretap Act . . . focus on the use of surveillance devices for acquisition.").

59. *Id.* The SCA does include a provision that prohibits the companies that store data from knowingly selling it to the government. *See infra* Part. III.A.

through Locate X, another location-tracking technology.[60] United States Special Operations Commands ("USSOCOM"), a U.S. military unit and a buyer and user of Locate X, is responsible for counterterrorism, counter-intelligence, and special reconnaissance.[61] USSOCOM has made affirmative statements that their data acquisition primarily targeted foreigners abroad, ostensibly in support of their larger counterterrorism and national security objectives.[62] Courts are likely to find national security-adjacent rationales persuasive.[63]

Historically, the law provides greater leeway to government national security actions, even in cases concerning privacy.[64] For example, the majority opinion in *Katz* includes a footnote that the decision does not reach national security matters.[65] In his concurrence, Justice White also acknowledged that "there are circumstances in which it is reasonable to search without a warrant" and that the decision "does not reach national

60. *How the U.S. Military Buys Location Data*, *supra* note 5; *see* Levinson, *supra* note 9 (explaining how Locate X is used by U.S. government agencies).

61. *How the U.S. Military Buys Location Data*, *supra* note 5.

62. *See id.*

63. *See* Shirin Sinnar, *Courts Have Been Hiding Behind National Security for Too Long*, BRENNAN CTR. FOR JUST. (Aug. 11, 2021), https://www.brennancenter.org/our-work/analysis-opinion/courts-have-been-hiding-behind-national-security-too-long [https://perma.cc/NK3W-XKF9] (citing a series of decisions evidencing courts' deference to national security rationales that limit court's jurisdictional authority, reduce the standard of review, or defer to factual conclusions by the executive); *see, e.g.*, Clapper v. Amnesty Int'l USA, 568 U.S. 398, 398 (2013) (holding that attorneys and human right organizations that engaged in sensitive and occasional privileged communications with people abroad lacked standing to challenge an electronic surveillance program under the FISA due to no traceable injury, despite amici reporting that the Government was expanding their electronic surveillance programs); Ziglar v. Abbasi, 137 S. Ct. 1843, 1849 (2017) (holding that the post-9/11 immigrant detainees could not sue government officials for damages for constitutional violations as a *Bivens* claim, because "special factors" counseled against such an action, specifically citing courts' reluctance to "intrude upon" what Congress and the Executive have determined to be "essential to national security").

64 *See, e.g.*, In re Opinions & Orders of the FISC Containing Novel or Significant Interpretations of Law, No. Misc. 20-02, 2020 WL 6888073, (FISA Ct. Rev., Nov. 19, 2020), *cert. denied*, 142 S.Ct. 22 (2021) (challenging the Foreign Intelligence Surveillance Court's refusal to grant public access to their decisions). Dissenting from the denial of certiorari, Justices Neil Gorsuch and Sonia Sotomayor underscored the "profound implications for Americans' privacy and their rights to speak and associate freely" affected by decisions of the Foreign Intelligence Surveillance Court. Am. C.L. Union v. United States, 142 S.Ct. 22, 2 (2021) (Gorsuch, J., dissenting). They also expressed shock at the government's argument that "literally *no court* in this country," including the Supreme Court, "has the power to decide whether citizens possess a First Amendment right of access to the work of our national security courts." *Id.* at 3 (Gorsuch, J., dissenting) (emphasis in original).

65. Katz v. United States, 389 U.S. 347, 358 n.23 (1967).

security cases."[66] Additionally, in his *Carpenter* opinion, Chief Justice Roberts declared that the judgment was narrow and "[did] not consider other collection techniques involving foreign affairs or national security."[67]

As a statutory matter, *Carpenter* and other Fourth Amendment protections do not extend to the extraterritorial searches of non-citizens. [68] FISA Section 702 permits the government to conduct warrantless domestic surveillance of electronic communications on "persons reasonably believed to be located outside the United States to acquire foreign intelligence information."[69] The Court has even found that "the 'incidental collection' of communications is permissible under the Fourth Amendment."[70] Therefore, if USSOCOM can establish that it is exclusively purchasing location data abroad, then it will be operating outside of *Carpenter*'s scope.

B. Remaining Questions and the Impact on Privacy

Depending on the actual data being acquired, the legal reality briefly explored above could insulate USSOCOM from claims of constitutional violations of the Fourth Amendment. However, that leaves open the question of why USSOCOM and other government agencies are purchasing this data when there is a myriad of other legal methods they could use to collect pertinent national security or counterterrorism data without raising *Carpenter* concerns. As aforementioned, if the government is principally seeking location data about foreigners, it could seek a FISA order to collect evidence so long as intelligence was a "significant" purpose.[71] Although the government would still need to obtain a Section 215 order from the Foreign Intelligence Surveillance Court, it would not have to demonstrate probable cause.[72]

---

66. *Id.* at 363 (White J., concurring).

67. Carpenter v. United States, 138 S. Ct. 2206, 2210 (2018).

68. *See* United States v. Verdugo-Urquidez, 494 U.S. 259, 261, 274 (1990) (considering the constitutionality of a search of a Mexican citizen by the DEA, the Court held that the Fourth Amendment does not apply to the search and seizure by property located in a foreign country and owned by a nonresident alien).

69. Foreign Intelligence Surveillance Act, 50 U.S.C. § 1881a; USA Patriot Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, 120 Stat. 192.

70. Incidental collection is defined as "the collection of the communications of individuals in the United States acquired in the course of the surveillance of individuals without ties to the United States and located abroad." United States v. Hasbajrami, 945 F.3d 641, 646 (2d Cir. 2019).

71. Letter from Stephen E. Boyd, Off. of the Assistant Att'y Gen., to Michael R. Pence, Vice President of the U.S. (July 17, 2020), https://www.justice.gov/nsd/nsd-foia-library/2019fisa/download [https://perma.cc/SM9E-BQDN].

72. *Id.*

If the data is being acquired for intelligence purposes, it could be collected through a National Security Letter ("NSL"). An NSL can be issued directly by commanding officers stationed across the country at FBI field offices, such as the FBI Director, an Assistant Director, or a FBI Special Agent in Charge. [73] Under the four relevant NSL-authorizing statutes, the government can issue NSLs to communications providers, financial institutions, consumer credit agencies, and travel agencies. [74] The government has interpreted these categories broadly. For example, the FBI has served NSLs on both a physical consortium of libraries and a digital library.[75] Although the statutory text does limit the type of information that can be requested, the FBI could still request information from someone who is not subject to an investigation so long as the information is relevant to an "investigation to protect against terrorism or clandestine intelligence activities."[76]

Additionally, Executive Order 12333 ("E.O. 12333") authorizes intelligence agencies to "collect, retain or disseminate information concerning United States persons," including "[i]nformation obtained in the course of a lawful foreign intelligence, counterintelligence, international narcotics or international terrorism investigation."[77] Therefore, if USSOCOM and other government agencies want to acquire foreigners' location data or data relevant to ongoing intelligence or counterterrorism operations, they could use other legal channels.[78]

In response to questions regarding their data purchases, the Navy Commander for USSOCOM stated that "[their] access to the [location data software] is used to support Special Operations Forces mission requirements overseas," and that they "strictly adhere to established procedures and policies for protecting the privacy, civil liberties, and constitutional and legal

---

73. 18 U.S.C. § 2709(b).

74. 18 U.S.C. § 2709 (concerning wire or electronic communication providers); 12 U.S.C. § 3414 (concerning financial institutions and records); 15 U.S.C. § 1681 (concerning credit agencies); 50 U.S.C. § 3162 (concerning travel agencies).

75. *See* Doe v. Gonzales, 449 F.3d 415, 417 (2d Cir. 2006) (concerning the FBI's demand of patron records via a section 2709 NSL, as expanded from the Patriot Act, from the Library Connection, a consortium of 26 Connecticut public libraries); Doe v. Mukasey, 549 F.3d 861, 861(2d Cir. 2008) (concerning an attempt by the federal government to use a Section 2709 NSL to access information held on Connecticut library servers).

76. 18 U.S.C. § 2709(b)(1–2).

77. Exec. Order No.12333, United States Intelligence Activities, 3 C.F.R. 59,941, 59950–51 (Dec. 4, 1981), *as amended by* Exec. Order 13470, 3 C.F.R. 218 (July 30, 2008).

78. This Part is not intended to include an exhaustive list of the powers at the government's disposal. Rather, it is intended to demonstrate that there are multiple legal ways in which the government could gain data of this type.

rights of American citizens."[79] However, it seems unlikely that USSOCOM is able to perfectly distinguish between foreigners and citizens, especially when the data is anonymized and acquired at such a massive volume.[80] Moreover, in their purchase of location data, CBP officials have said that they are not "attempt[ing] to distinguish between the data of Americans and foreign nationals."[81]

With other options available, it is worth asking why government agencies chose this route. Perhaps the commercial purchase pathway permits agencies such as USSOCOM to build a massive database of location data that would be otherwise impossible to acquire, especially since some courts have found that querying databases of stored information acquired under FISA could function as a separate Fourth Amendment search requiring a reasonability analysis.[82] In *Carpenter*, the Justices were troubled by the government's ability to acquire a historic, massive database through which they could track an individual's movements.[83] Most importantly, even when location records are generated for commercial purposes, an individual's "anticipation of privacy in his [or her] physical location" is not negated.[84] No matter how the government obtains the data, the impact on privacy remains, heightened by the secrecy provisions embedded in many of these data brokers' terms and conditions and the reticence of the agencies themselves to respond to calls for transparency.[85]

Finally, even if these data purchases are actually related to national security and counterterrorism, their extra-constitutional nature remains problematic. In his *Katz* concurrence, Justice Douglas worried about giving the Executive Branch and its composite agencies a greenlight to resort to various and otherwise illegal measures in the name of national security.[86] The Justice's words resonate even more forcefully in light of a recently exposed secret CIA bulk collection program.

---

79. *How the U.S. Military Buys Location Data*, *supra* note 5.

80. *Apps Are Selling Your Location Data. The U.S. Government Is Buying*, *supra* note 2.

81. Drew Harwell, *Senators Seek IG Probe of Border Agency's Warrantless Use of Phone Location Data*, WASH. POST (Oct. 23, 2020), https://www.washingtonpost.com/technology/2020/10/23/warrantless-cbp-phone-data-searches/ [https://perma.cc/DW9J-AK74].

82. United States v. Hasbajrami, 945 F.3d 641, 669–73 (2d Cir. 2019).

83. Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018) ("With just the click of a button, the Government can access each carrier's deep repository of historical location information at practically no expense.").

84. *Id.*

85. Levinson, *supra* note 9.

86. Katz v. United States, 389 U.S. 347, 359–60 (Douglas, J., concurring).

In April 2021, Senators Ron Wyden and Martin Heinrich sent a letter to the Director of National Intelligence and to the Central Intelligence Agency ("CIA"), requesting expedited declassification of the Privacy and Civil Liberties Oversight Board's ("PCLOB") "Executive Order 12333 Central Intelligence Agency Deep Dive II."[87] Despite clear historic and continued congressional intent to "limit and . . . prohibit the warrantless collection of Americans' records," the Senators state that the CIA's secret collection has occurred outside the appropriate statutory framework, absent any oversight, and without public transparency.[88]

On February 10, 2022, the PCLOB released its heavily redacted seventy-one-page report on "CIA Financial Data Activities in Support of ISIL-Related Counterterrorism Efforts," accompanied by a portion of the PCLOB Staff Recommendations.[89] Although the PCLOB's report centers on data collections directed against non-U.S. entities and persons pursuant to E.O. 12333,[90] the Report evaluated the adequacy of the CIA's procedures on the incidental collection of the data of Americans abroad. Importantly, the PCLOB Report finds that, although some CIA policies exist on the collection, retention, and dissemination of citizen data, "[they] do not directly address key aspects of handling and use—activities that impact the privacy of [U.S. persons] whose information has been collected incidentally."[91]

Allegedly, when attempting to use citizen information collected under the bulk data scheme, CIA analysts are prompted with a pop-up reminding them that they need a foreign intelligence purpose to query such data.[92] However, this pop-up does not require CIA analysts to record their specific foreign intelligence purpose, nor does it analyze offered access

---

87 *See* Letter from Sen. Ron Wyden, et al., to Hon. Avril Haines, Director of National Intelligence, Hon. William J. Burns, Director of Central Intelligence Agency, (Apr. 13, 2021), https://www.wyden.senate.gov/imo/media/doc/HainesBurns_WydenHeinrich_13APR21%20-FINAL.pdf [https://perma.cc/8NGZ-9SXJ].

88 *Id.* at 2.

89 Report on CIA Financial Data Activities in Support of ISIL-Related *Counterterorrism [sic] Efforts*, U.S. PRIV. & C.L. OVERSIGHT BD., https://www.cia.gov/static/63f697addbbd30a4d64432ff28bbc6d6/OPCL-PCLOB-Report-on-CIA-Activities.pdf [https://perma.cc/CRA9-NMVE] [hereinafter *CIA Report*]; *see also (U) Recommendations from PCLOB Staff*, U.S. PRIV. & C.L. OVERSIGHT BD., https://www.cia.gov/static/f61ca00cbcda9b5d46a04e0b53b5f2b9/OPCL-Recommendations-from-PCLOB-Staff.pdf [https://perma.cc/R97B-HUMP] [hereinafter *PCLOB Recommendations*] (describing six different recommendations to improve the CIA's Attorney General Guidelines).

90 *CIA Report*, *supra* note 89, at 11.

91 *CIA Report*, *supra* note 89, at 62.

92 *PCLOB Recommendations*, *supra* note 89, at 1.

justifications.[93] Consequently, it is incredibly difficult to review or audit agents' justifications for using U.S. citizen data.[94] In response, the PCLOB recommends "requir[ing] analysts to provide a written justification for [U.S. persons] queries."[95]

The lacuna of policy governing the incidental bulk collection under E.O. 12333 actions, combined with the CIA's unwillingness to disclose their activities, demonstrates the preeminence of national security rationale over privacy considerations. Clearly, government agencies acting under the auspices of national security are already circumventing existing procedures intended to safeguard Americans and their constitutional rights.

In light of these disclosures, permitting the government to further end-run *Carpenter* and the Fourth Amendment through commercial data acquisitions ostensibly for national security or counterterrorism reasons, even in a situation absent a statute or ruling, undermines the very principles articulated in *Carpenter*.[96] For the Muslim American community, these revelations are just the latest in a string of privacy violations justified by national security reasons. The purchase of this location data may lead to action against the Muslim community both domestically and abroad.[97]

---

93 *PCLOB Recommendations*, *supra* note 89, at 2 (recommending the CIA implement a program to better address data retention and consider adopting automated tools to assist with compliance).

94 *PCLOB Recommendations*, *supra* note 89, at 1.

95 *Id.* The PCLOB also recommends that the CIA develops a strategy on data retention and use of historic datasets that may include the information of citizens. *Id.* at 2. This type of query is exactly what the Second Circuit said is necessary to satisfy Fourth Amendment protections in the case data stored pursuant to Section 702 of FISA. See United States v. Hasbajrami, 945 F.3d 641, 670–73 (2d Cir. 2019).

96. Cat Zakrzewski, *The Technology 202: ACLU Sues DHS over Purchase of Cellphone Location Data Used to Track Immigrants*, WASH. POST (Dec. 2, 2020), https://www.washingtonpost.com/politics/2020/12/02/technology-202-aclu-sues-dhs-over-purchase-cellphone-location-data-used-track-immigrants/ [https://perma.cc/5G8S-XUB7].

97. The government allegedly uses meta and location data to conduct drone strikes abroad. *Action Alert: Call for Congressional Hearing on Military Reportedly Spying on Muslims Using Data from Religious Apps*, COUNCIL ON AMERICAN-ISLAMIC RELS. (Nov. 16, 2020), https://www.cair.com/press_releases/action-alert-cair-condemns-government-for-reportedly-spying-on-muslims-using-data-from-religious-apps-calls-for-congressional-inquiry/ [https://perma.cc/PU7X-JZYD] (calling for a congressional hearing in light of the confirmation by the government that enforcement agencies are acquiring and using personal data targeting the Muslim community); Jordan Pearson, *The Problem with Using Metadata to Justify Drone Strikes*, VICE (Oct. 15, 2015), https://www.vice.com/en/article/3da8n9/the-problem-with-using-metadata-to-justify-drone-strikes [https://perma.cc/B8XE-CE6Q] (reporting that the U.S. military is over-reliant on signals intelligence ("SIGINT") such as cell phone records that include call times and the content of phone and online communications when selecting drone strike targets).

Stateside, the sale of this information evokes memories of post-9/11 New York City Police Department surveillance efforts to physically map Muslim communities and build expansive intelligence databases that included the names of thousands of innocent New Yorkers.[98] The asymmetry between government enforcement agencies' behavior and *Carpenter*, as well as the impact these purchases have on privacy and civil society, cannot be overstated.

III. Potential Remedies

Faced with this legal uncertainty, users and legislators have a few options to fortify their Fourth Amendment protections. While specific information about the Muslim Pro location dataset is still wanting, the ACLU has filed a recent FOIA request to learn more about the specifics of the government agencies' purchases of Muslim Pro and other applications' data from X-Mode and Locate X.[99] The clarity provided by this information will help users and legislators ascertain the scope of the damage and subsequently evaluate which actions will prove the most fruitful.

A. Company-Led Solutions

One possibility is that users could rely on the goodwill of big technology companies to enforce their privacy rights. In December 2020, Google and Apple announced a joint ban on X-Mode's tracking software.[100] To comply, developers either had to remove X-Mode's embedded SDKs or risk losing access to the mobile phone giants' application store and mobile operating systems.[101] In response, in August 2021, X-Mode was acquired by the IP Intelligence company Digital Envoy, with plans to rebrand as

---

98. *See Factsheet: The NYPD Muslim Surveillance Program*, ACLU, https://www.aclu.org/other/factsheet-nypd-muslim-surveillance-program [https://perma.cc/F2UV-MUR3] (outlining how the New York Police Department has been surveilling the Muslims in New York and the greater area since 2002 through its Demographics Unit (renamed the Zone Surveillance Unit), the Intelligence Analysis Unit, the Cyber Intelligence Unit, and the Terrorist Interdiction Unit).

99. *ACLU, CLEAR FOIA Request Concerning Purchase and Use of Cell Phone Location Data*, *supra* note 4.

100. Bryon Tau, *Apple and Google to Stop X-Mode from Collecting Location Data from Users' Phones*, WALL ST. J. (Dec. 9, 2020), https://www.wsj.com/articles/apple-and-google-to-stop-x-mode-from-collecting-location-data-from-users-phones-11607549061 (on file with *Columbia Human Rights Law Review*).

101. *Id.*; Bennett Cyphers, *App Stores Have Kicked Out Some Location Data Brokers. Good, Now Kick Them All Out*, ELEC. FRONTIER FOUND. (Mar. 10, 2021), https://www.eff.org/deeplinks/2021/03/apple-and-google-kicked-two-location-data-brokers-out-their-app-stores-good-now [https://perma.cc/7WF8-CQ5K].

Outlogic.[102] Digital Envoy stated that, as part of the purchase, it would end the sale of U.S. location data to defense contractors.[103]

Yet, anointing private companies as white knights is an incomplete, and potentially deleterious, strategy. On a practical level, because Google and Apple's punitive approach is reactive, it does not stop tracking software of this type from proliferating. The ban of one—or even a few—data brokers does not function as a death sentence for the entire industry, especially with stable demand from government agencies for data.[104]

Depending on large companies like Google and Apple dangerously strengthens a digital privacy regime in which private, profit-seeking companies determine how and when to enforce users' constitutionally provided Fourth Amendment rights and universal human rights. Today, private companies neither premised on, nor founded to protect constitutional, human, or civil rights, are elevated to be defenders and arbiters of those rights—even though rights protection may run perpendicular to commercial gain.[105] In other words, the whim of companies

---

102. Laurie Sullivan, *Location-Data Broker X-Mode Acquired by Digital Envoy,* MEDIA POST (Aug. 4, 2021), https://www.mediapost.com/publications/article/365693/location-data-broker-x-mode-acquired-by-digital-en.html [https://perma.cc/H9P8-VSXW].

103. Michaela Althouse, *Reston's X-Mode Is Rebranding as Outlogic and Upping Its Data Ethics Following an Acquisition by Atlanta's Digital Envoy*, TECHNICAL.LY (Aug. 5, 2021), https://technical.ly/dc/2021/08/05/x-mode-digital-envoy/ [https://perma.cc/H8BL-YSKG].

104. For example, in June 2021, Google banned SafeGraph, a location data broker that uses a similar SDK model to X-Mode, from its application store for violating anonymity provisions. SafeGraph data was used by the N.Y. Times to detail how easy it is to deanonymize allegedly anonymous data. Joseph Cox, *Google Bans Location Data Firm Funded by Former Saudi Intelligence Head*, VICE (Aug. 12, 2021) https://www.vice.com/en/article/5db4ad/google-bans-safegraph-former-saudi-intelligence [https://perma.cc/YHU2-ALDS]. Prior to the ban, the Illinois Department of Transportation ("IDOT") had purchased geolocation data from SafeGraph that covered over 40% of the state's population. Even with SafeGraph's ban, if IDOT and other state and federal government agencies want to access similar bulk location data, there are various data brokers from which to do so, including HERE Data LLC and Replica. Bennett Cyphers & Jason Kelley, *Illinois Bought Invasive Phone Location Data from Banned Broker Safegraph*, ELEC. FRONTIER FOUND. (Aug. 19, 2021), https://www.eff.org/deeplinks/2021/08/illinois-bought-invasive-phone-location-data-banned-broker-safegraph [https://perma.cc/JM4D-QQ47]. Thus, case-by-case bans by Google and Apple are essentially a game of whack-a-mole because new data brokers constantly rise to meet market demands.

105 Kate Klonick, *The New Governors: The People, Rules, and Processes Governing Online Speech*, 131 HARV. L. REV. 1598, 1603 (2018); see also Evelyn Douek, *The Rise of Content Cartels*, KNIGHT FIRST AMEND. INST. AT COLUM. UNI., (Feb. 11, 2020), https://knightcolumbia.org/content/the-rise-of-content-cartels [https://perma.cc/E66W-BHZC] (discussing the tension between the protection of user data and free

primarily oriented towards profit currently determines the contours of user data protection. Leaning on big private companies only reinforces their monopolistic influence in the technology space, rendering them increasingly ubiquitous and omnipotent, and difficult to regulate.

B. Legal Remedies for Muslim Pro Users

Muslim Pro Users themselves could seek legal remedy for the violations of their constitutional rights. Users could explore the possibility of suit against the government under *Carpenter* itself. Professor Orin Kerr argues that the Court's decision in *Carpenter* can be understood under the theory of equilibrium-adjustment, which states that "[w]hen technology dramatically expands the government's power under an old legal rule, the thinking goes, the Court changes the legal rule to restore the prior level of government power."[106] This parallels Chief Justice Roberts' writings that, in determining the boundaries of reasonableness and privacy, the Court "must take account of more sophisticated systems that are already in use or in development."[107]

Professor Orin Kerr argues that, in its determination of whether and where a search occurred, the *Carpenter* Court was more concerned with the fact that the government ended up with too much information than the exact means by which the government acquired that information.[108] Applying this reasoning to the Muslim Pro case, a creative lawyer could first establish that the government and the military do currently have access to the bulk location data, which could be done using media reports and results from the ACLU FOIA request. With proof of government possession of CSLI in hand, a lawyer would then argue that this information is the "product of a search," just like the data turned over from wireless carriers which the *Carpenter* Court determined needed a warrant.[109] Despite no specific place, person, or thing having been searched, a U.S. agency's purchase and retention of CSLI could be evidence that, somewhere along the chain of acquisition, an improper search occurred.[110] Because what matters for a *Carpenter* search is the final possession of the information, rather than the specific process of acquisition,

---

speech, and cooperation with governmental bodies to combat crimes such as child pornography).

106. Orin Kerr, *When Does a Carpenter Search Start – and When Does It Stop?*, LAWFARE (July 6, 2018), https://www.lawfareblog.com/when-does-carpenter-search-start-and-when-does-it-stop [https://perma.cc/SGX4-WV6S].

107. Carpenter v. United States, 138 S. Ct. 2206, 2210 (2018) (quoting Kyllo v. United States, 533 U.S. 27, 36 (2001))

108. Kerr, *supra* note 106.

109. *Id.*

110. *Id.*

the facts support an argument that an agency's purchase of this data mirrors the unconstitutional warrantless requests of CSLI from wireless carries and thus violates *Carpenter*.

Beyond arguing a *Carpenter* violation, Muslim Pro users have at least two other pathways to a remedy. According to the SCA, companies that store and transmit user data are generally prohibited from "knowingly" sharing those records with the government.[111] In a recent public advisory, Muslim Pro denied selling users' personal data to the U.S. military, although it did admit that it had shared anonymized data with "selected technology partners who are required to comply with global laws and regulations around data privacy protection."[112] If users could establish that Muslim Pro knew that, further down the commercial chain, data generated from the application was being divulged to the government, they could file suit under the SCA.[113]

Muslim Pro users could also follow the lead of customers of The Weather Channel ("TWC") application and bring a class action lawsuit. In their complaint, plaintiffs in *People v. TWC* argued that TWC "deceptively used its Weather Channel App" to mine its users' geolocation data without true voluntary consent and with the aim of "using [the data] and monetizing it for purposes entirely unrelated to weather or the Weather Channel App." [114] Similar to the Muslim Pro case, *TWC* plaintiffs allege that the application's privacy policy and privacy settings did not include a disclosure that explained the purposes of the tracking of geolocation data, or that TWC was planning on sharing that data with third parties for non-weather related reasons.[115] It remains to be seen how the *TWC* case is treated in court, but one potential hurdle for Muslim Pro users is that they may have to establish that, like TWC, the core business for Muslim Pro was to "amass[] and profit[] from user location data."[116] By arguing that a company's core business is focused on the aggregation and sale of user data, yet it fails to inform or

111. 18 U.S.C § 2703; Edelman, *supra* note 9.

112. Muslim Pro has also terminated its relationship with X-Mode. Muslim Pro Official (@MuslimPro), TWITTER (Nov. 17, 2020, 8:50 AM), https://twitter.com/MuslimPro/status/1328697072665628673/photo/1 [https://perma.cc/ZG87-W3CQ].

113. Edelman, *supra* note 9; Levinson, *supra* note 9.

114. Complaint for Injunctive Relief and Civil Penalties at 1, *People v. TWC*, No. 19STCV00605, 2020 Cal. Super. LEXIS 157* (CA Super. Ct., LA Cnty., Aug. 14, 2020), https://src.bna.com/EqH [https://perma.cc/4J3K-JJ3Y].

115. *Id.* at 3–4.

116. *Id.* at 1.

misleads the consumer, plaintiffs could have an arguable violation of unfair competition law.[117]

C. Federal and State Legislative Solutions

In an ideal world, the reasonable expectation of privacy standard could be codified into statutory law. In his *Riley* concurrence, Justice Alito identified that "[l]egislatures, elected by the people, are in a better position than we are to assess and respond to the changes that have already occurred and those that almost certainly will take place in the future."[118] Absent statutory protection, citizens often have to rely on the prudence of governmental agencies and bureaucracy to limit their own surveillance powers.[119] Fortunately, legislatures on Capitol Hill and in statehouses are working to eliminate the grey area exposed by the Muslim Pro case.

At the federal level, Senator Wyden has proposed a bill entitled "The Fourth Amendment is Not for Sale Act," which would prohibit law enforcement agencies from circumventing the normal *Carpenter* warrant process by buying information from commercial data brokers.[120] The bill

---

117. While the *TWC* case argues a violation of California's Unfair Competition Law, a federal complaint seeking an injunction and/or damages could cite the federal Lanham Act section on false-advertising. The relevant language is as follows:

> Any person who, or in connection with any goods or services . . . uses in commerce any word, term, name, symbol, or device , or. . . false or misleading description of fact, or false or misleading representation of fact, which in commercial advertising or promotion, misrepresents the nature, characteristics, [or] qualities . . . of his or her . . . goods, services, or commercial activities.

18 U.S.C. § 1125(a)(1).

118. Riley v. California, 573 U.S. 373, 408 (2014) (Alito, J., concurring).

119. *Apps Are Selling Your Location Data. The U.S. Government Is Buying*, *supra* note 2.

120. Nilay Patel & Adi Robertson, *Donald Trump Trying to Control the FCC Is a 'Disaster' Says Sen. Ron Wyden*, THE VERGE (Aug. 4, 2020), https://www.theverge.com/2020/8/4/21354244/ron-wyden-fcc-nomination-section-230-trump-order-vergecast-interview [https://perma.cc/XC5R-AQ89]. The bill's text states it is intended to "prevent law enforcement and intelligence agencies from obtaining subscriber or customer records in exchange for anything of value, to address communications and records in the possession of intermediary internet service providers, and for other purposes." The Fourth Amendment Is Not for Sale Act, S. 1265, 117th Cong. (1st Sess. 2021), https://www.congress.gov/117/bills/s1265/BILLS-117s1265is.pdf (last visited Feb. 24, 2022). A companion bill in the House of Representatives was introduced by Congresspeople Jerrold Nadler and Zoe Lofgren in April, 2021. *Nadler, Lofgren Introduce Bicameral Fourth Amendment Is Not for Sale Act*, LOFGREN PRESS RELEASES (Apr. 21, 2021), https://lofgren.house.gov/media/press-releases/nadler-lofgren-intro-bicameral-fourth-amendment-not-sale-act [https://perma.cc/4THV-FJ6K]. The bill is supported by major

includes language that would also stop the indirect acquisition of records and information by government agencies from third parties, as well as the sharing of information between non-law enforcement or intelligence agencies with law enforcement.[121] Finally, the bill specifies that courts must apply "the most stringent standard" when deciding whether to require a third party to disclose customer information to a government agency.[122]

Senator Wyden identified the legislation's central purpose as forcing technology and data-broker company CEOs to take privacy seriously.[123] Speaking about the need for this bill, he said, "I don't think Americans' Constitutional rights ought to vanish when the government uses a credit card instead of a court order."[124] Similarly, on the Senate floor, he insisted that "it is especially important that the American people are told if the government is using legal loopholes in the law and the warrant requirement of the Fourth Amendment."[125]

Congressional deadlock may hamper or delay the passage of Senator Wyden's bill.[126] However, recently legislatures have proposed several state-

---

privacy activists and human rights organizations. *See* Letter from the ACLU et al., *Congress Must Restore Constitutional Limits on Surveillance*, BRENNAN CTR. FOR JUST. (Feb. 16, 2021), https://www.brennancenter.org/sites/default/files/2021-03/Surveillance%20Briefer%202.16.21.pdf [https://perma.cc/QGH2-TSEW].

121. S. 1265, §§ 2(2)(A–B).

122. *Id.* § 3(3)(B).

123. Patel & Robertson, *supra* note 120.

124. *Id.*

125. Senator Ron Wyden, *Remarks Before the Confirmation Vote for Director of National Intelligence Avril Haines*, C-SPAN (Jan. 21, 2021), https://www.c-span.org/video/?c4940346/user-clip-sen-wyden-purchase-americans-data-dni-haines [https://perma.cc/AK3P-82CV]. Senator Wyden also explicitly asked Director Haines about the government purchase of private records from commercial data brokers, like X-Mode.

126. Senator Wyden introduced his bill along with a group of 19 bipartisan senators, including Senator Rand Paul. Senator Wyden's bill, and its identical counterpart in the House, were both introduced in April 2021. The House bill has been referred to the Subcommittee on Crime, Terrorism, and Homeland Security. The Senate bill has been read twice and referred to the Committee on the Judiciary. *H.R. 2738 – Fourth Amendment Is Not for Sale Act: Overview,* CONGRESS.GOV, https://www.congress.gov/bill/117th-congress/house-bill/2738/ (last visited Feb. 24, 2022) (noting the bill's referral to subcommittee on October 19, 2021); *S. 1265 – Fourth Amendment Is Not for Sale Act: Overview*, CONGRESS.GOV, https://www.congress.gov/bill/117th-congress/senate-bill/1265/ (last visited Feb. 24, 2022) (noting the bill's introduction and referral to the Senate Judiciary on April 21, 2021, with no subsequent subcommittee referrals as of Feb. 24, 2022). On January 26, 2022, a coalition of privacy, free speech, civil rights, and civil liberties groups sent a letter to both Representative Nadler and Senator Durbin, the chairs of their respective Judiciary Committees, demanding hearings on the bills. Letter from Access Now et al., to Hon. Dick Durbin, Chair of Senate Judiciary Comm., Hon. Chuck Grassley, Ranking Member of Senate Judiciary Comm., Hon. Jerry Nadler, Chair of House

level initiatives to improve the protection of consumer data.[127] While these bills would not have prohibited the sale of data to federal actors in the Muslim Pro case, they are an important step in the right direction. One success occurred in March 2019 when Utah passed a groundbreaking law entitled the "Electronic Information or Data Privacy Act" ("H.B. 57").[128] H.B. 57 requires law enforcement to obtain a warrant upon probable cause before accessing "location information, stored data, or transmitted data" of "electronic information or data transmitted by the owner of the electronic information or data to a remote computing service provider."[129] H.B. 57 also includes a notification requirement; after obtaining a warrant, law enforcement must notify the owner of the electronic device, information, or data within a delineated timeframe.[130]

Statutes like H.B. 57 reflect the fluidity of mainstream understanding of reasonable government access and privacy. They speak to what society deems as reasonable, filling in the gaps left by federal statutes and judge-made doctrines. Hopefully, statutes of this kind proliferate at a state level and, in tandem with Senator Wyden's bill, provide clear guidance to protect against this new type of privacy invasion by governmental officials.

Judiciary Comm., & Hon. Chuck Grassley, Ranking Member of House Judiciary Comm. (Jan. 26, 2022), https://www.freepress.net/sites/default/files/2022-01/final_-_fanfsa_sign-on_letter_january_2022.pdf [https://perma.cc/5LL7-23FX]. As of this publication, no hearings had yet been scheduled.

127. *See generally* California Consumer Privacy Act of 2018 (CCPA), CAL. CIV. CODE §§ 1798.100–1798.196 (West 2022) (giving California consumers the right to know what data a business collects and how it is used, the right to delete personal information, the right to opt-out of sale of their personal information, and the right to non-discrimination for exercising these CCPA rights); Colorado Privacy Act, COLO. REV. STAT. ANN. §§ 6-1-1301–6-1-1313 (effective July 1, 2023) (addressing consumers' right to privacy, companies responsibility to protect personal data, and authorizing the Attorney General and district attorney to take enforcement action for violations); Virginia Consumer Data Protection Act, VA. CODE ANN. §§ 59.1.575–59.1585 (2021) (effective Jan. 1, 2023) (addressing the responsibilities and privacy protection standards for data controllers and processors and giving exclusive authority to the Attorney General to enforce, modeled after frameworks used in earlier California legislation and the European Union's General Data Protection Regulation ("GDPR")).

128. Molly Davis, *Utah Just Became a Leader in Digital Privacy*, WIRED (Mar. 22, 2019), https://www.wired.com/story/utah-digital-privacy-legislation/ [https://perma.cc/SY7J-JN42].

129. *Id.*; Electronic Information or Data Privacy, UTAH CODE ANN. §§ 77–23c–101, 77–23c–102, 77–23c–103 (West 2019), https://le.utah.gov/~2019/bills/static/HB0057.html [https://perma.cc/8FG8-B48W].

130. Electronic Information or Data Privacy, UTAH CODE ANN. § 77-23c-103 (West 2019).

CONCLUSION

"Setting the Fourth Amendment right is part of standing up . . . . for fairness in our society." [131] In a world increasingly dependent on technological devices and applications constantly collecting information, "individuals have no realistic alternative" and cannot be considered to legitimately assume the risks associated with their essential devices.[132] If the loophole exposed by this case is not filled, then, "legitimate privacy rights [will be left] at the 'mercy of advancing technology.'"[133]

Surveillance policy must balance between community and individual liberty and privacy interests, and the government interest in protecting the public and fighting crime. However, that balance has fallen unfairly on marginalized communities. The Muslim American community in particular has been subject to targeted and expansive government surveillance justified by broad national security reasons. Even against this unequal baseline, the Fourth Amendment and the third-party doctrine, as understood by *Carpenter*, safeguards society's privacy interests by recognizing that reasonable expectations of privacy shift accordingly with increased technological innovation.

Permitting commercial purchases of location data that would otherwise require a warrant undermines the spirit of privacy law, tipping the balance decisively in favor of the government over civil liberties. As evident from the Muslim Pro case and others, the circumvention of *Carpenter* and the Fourth Amendment also lacks transparency and legal certainty, leaving the public in the dark as to how their data is being catalogued and searched.

The COVID-19 pandemic has elevated the saliency of location data.[134] With more location data available than ever before, and with the government empowered to acquire that data through multiple pathways of varying legality, establishing clear regulations is essential. The Fourth Amendment should not be treated as an irritating impasse, around which

---

131. How to Fix the Internet*, Fixing a Digital Loophole in the Fourth Amendment*, ELEC. FRONTIER FOUND. at 24:06 (Nov. 17, 2020), https://www.eff.org/deeplinks/2020/11/podcast-episode-fixing-digital-loophole-fourth-amendment [https://perma.cc/N39N-5RYL].

132. Smith v. Maryland, 442 U.S. 735, 749–50 (1979) (Marshall, J., dissenting).

133. Commonwealth v. Almonor, 120 N.E.3d 1183, 1196 (2019) (quoting Kyllo v. United States, 533 U.S. 27, 34–35 (2001)).

134. For example, X-Mode is currently using location data to track potential COVID hotspots. Joseph Green, *Location Data in Action: X-Mode Tracks Potential COVID Hotspots Across the U.S.*, XMODE.IO, https://xmode.io/location-data-in-action-x-mode-tracks-potential-covid-hotspots-across-the-us/ [https://perma.cc/7SLM-EPVN].

data purchases on the open market provide a detour—the protections it enshrines are more fundamental and important than that.