Harvard Journal of Law & Technology
Volume 31, Number 1 Fall 2017

EQUAL ACCESS TO PUBLIC COMMUNICATIONS DATA FOR SOCIAL MEDIA SURVEILLANCE SOFTWARE

*Christopher L. Izant**

TABLE OF CONTENTS

I. INTRODUCTION

A recent trend among popular social media companies is to change developer policies to prohibit surveillance uses of data collected by the companies.[1] Enhanced social media surveillance capabilities made possible by data aggregation and analysis may reduce some practical obscurity for users who post publicly, but the ability to view and organize this

* Harvard Law School & Harvard Kennedy School, Candidate for J.D. & M.P.P., 2018; B.A. Boston College, 2010. I would like to thank Professor Jonathan Zittrain for his initial guidance and input that led to this Note, as well as Nati Hyojin Kim and the other editors of the Harvard Journal of Law and Technology, for all their work bringing this note to print. All opinions and errors are the author's own.

1. *See infra* Part IV.

data at the developer level is essential to capture the maximum intelligence value of social media communications. Social media companies with application programming interfaces ("APIs") should thus allow application developers who provide tools for government surveillance to access public communications data to the same degree as any other private software developer. Given the lawfulness of social media surveillance[2] and its critical intelligence value, legislation is needed to reverse the current trend of social media companies blocking access to developers who build applications for government surveillance.

This Note begins with a discussion of social media surveillance in Part II, highlighting the unique value of software built on access to APIs. Part III discusses the potential legal issues involved with government collection and analysis of public communications data. The recent trend of increased hostility between government agencies and social media companies and the potential consequences of this hostility are described in Part IV, with particular focus on changes to the software developer policies of Facebook and Twitter that restrict the use of their APIs for surveillance purposes. Acknowledging the futility of persuasion to convince social media companies to revert these policies, Part V proposes legislation to guarantee equal access to social media companies' APIs for developers who create surveillance applications for the government.

II. THE VALUE OF SOCIAL MEDIA SURVEILLANCE

As social media in particular has become a mainstream platform for public communications, its intelligence value has correspondingly increased, leading to both benefits and unintended harms.[3] Even a Supreme Court Justice has recently acknowledged that social media platforms provide both a ready means of committing crimes and a source of evidence.[4] Public posts can indicate threats to public safety,[5] which authorities (or friends and family) can use as a predicate for intervention

2. *See infra* Part III.

3. *See* Joel R. Reidenberg, *Privacy in Public*, 69 U. MIAMI L. REV. 141, 153 (2014) (discussing the insidious uses of publicly available information on social media as illustrated by "Girls Around Me," a website that scraped social media for women's pictures and real-time location information that were displayed on a map, which provided a handy tool for stalkers, and "PleaseRobMe.com," an application that identified likely vacant residences on a map based on social media posts that indicated homeowners were on vacation or at school).

4. *See* Elonis v. United States, 135 S. Ct. 2001, 2017 (2015) (Alito, J., concurring in part and dissenting in part) ("Threats of violence and intimidation are among the most favored weapons of domestic abusers, and the rise of social media has only made those tactics more commonplace.").

5. *See, e.g.*, *The Twitter Accounts of Dzhokhar Tsarnaev*, BOS. GLOBE (Mar. 10, 2015), https://www.bostonglobe.com/metro/2015/03/09/dzhokhar-tsarnaev-twitter-accounts/XJmVXtERqLwiYWwWxKw8lO/story.html (last visited Dec. 20, 2017).

or further investigation.[6] Crisis response agencies can respond in real time without having to divert scarce resources to collect reports from the field,[7] and social media platforms have even integrated helpful features in recognition of this crucial role.[8]

Law enforcement and intelligence agencies increasingly seek to exploit the value of social media through a range of techniques. Like other users, government agencies can employ simple techniques for monitoring social media, such as hashtag or term queries on the public-facing website interfaces.[9] They may also create fake accounts and request to connect with a target to gain access to private posts.[10] Success stories of using targeted social media surveillance, however, show that its applications are limited, that it takes significant time, and that it cannot provide comprehensive ways to search through and analyze public posts.[11] To conduct complex analyses and respond to events in real time, many police departments and intelligence agencies rely on access to data beneath the application layer of surveillance.[12]

Social media companies can grant commercial developers access to APIs so programmers can utilize the companies' protocols and data to build their own software.[13] APIs allow a developer access to raw data, where geolocation tags and precise temporal metadata may be readily available and integrated with other data types.[14] Some developers use

---

6. *See, e.g.*, Eric Lichtblau, *F.B.I. Steps up Use of Stings in ISIS Cases*, N.Y. TIMES (June 7, 2016), https://www.nytimes.com/2016/06/08/us/fbi-isis-terrorism-stings.html (last visited Dec. 20, 2017).

7. *See* Andrew V. Moshirnia, *Valuing Speech and Open Source Intelligence in the Face of Judicial Deference*, 4 HARV. NAT'L SEC. J. 385, 440–51 (2013) (discussing the role of social media APIs in crisis response); *see also* Deepa Seetharaman & Georgia Wells, *Hurricane Harvey Victims Turn to Social Media for Assistance*, WALL ST. J. (Aug. 29, 2017), https://www.wsj.com/articles/hurricane-harvey-victims-turn-to-social-media-for-assistance-1503999001 (last visited Dec. 20, 2017).

8. *See, e.g.*, *Safety Check*, FACEBOOK, https://www.facebook.com/about/safetycheck/ [https://perma.cc/34ME-YNEB].

9. *See, e.g.*, Zanders v. State, 73 N.E.3d 178, 180 (Ind. 2017) (discussing how defendant called liquor store to find out closing time before robbery; police entered phone number into Facebook search engine, leading to defendant's page where publicly posted video displayed fruits of robbery).

10. *See, e.g.*, Megan Behrman, *When Gangs Go Viral: Using Social Media and Surveillance Cameras to Enhance Gang Databases*, 29 HARV. J.L. & TECH. 315, 322 (2015) (discussing how police use fake social media profiles to conduct undercover gang investigations online).

11. *See id.*

12. JONATHAN ZITTRAIN, THE FUTURE OF THE INTERNET 67–68 (2008) (discussing architecture of the internet and its conceptual layers: the "physical layer," composed of the materials that transmit data such as fiber-optic cables and airwaves; the "protocol layer," where data is organized from electromagnetic pulses and transmitted according to computational instructions; and the "application layer," where users interface with the data, such as a website).

13. *Cf.* Oracle Am., Inc. v. Google Inc., 810 F. Supp. 2d 1002, 1007 (N.D. Cal. 2011).

14. *See* Mark Burdon, *Privacy Invasive Geo-Mashups: Privacy 2.0 and the Limits of First Generation Information Privacy Laws*, 2010 U. ILL. J.L. TECH. & POL'Y 1, 6 (2010) (attributing the growth of "geo-mashups" — applications that integrate geolocation metadata with other types of data — to the availability of APIs).

APIs to sort through and organize publicly available information for advanced database queries and analyses by law enforcement and intelligence agencies.[15] With a tool like Geofeedia, for example, a detective investigating a crime can enter specific location and temporal parameters to retrospectively view and search all the public posts on social media websites for which the tool has API access.[16] Alternatively, officials can use such software to monitor a specific event in real time and create automated alerts to identify threats to public safety.[17] The API-dependent capability to analyze vast amounts of public data is a crucially valuable tool for law enforcement and intelligence agencies. A former deputy director of the CIA explained that "tweets and other social media messages . . . often produce information that, especially in the aggregate, provides real intelligence value."[18] Without API-enabled social media software to aggregate and analyze public communications data, law enforcement and intelligence agencies could see another corner of the room "going dark."[19]

---

15. Such products include Digital Stakeout, Media Sonar, Dataminr, Geofeedia, X1 Social Discovery, and others. Nicole Ozer, *Police Use of Social Media Surveillance Software Is Escalating, and Activists Are in the Digital Crosshairs*, ACLU (Sept. 22, 2016), https://www.aclu.org/blog/privacy-technology/surveillance-technologies/police-use-social-media-surveillance-software [https://perma.cc/8LFG-VMU9].

16. *See generally Location-Based Intelligence Features*, GEOFEEDIA, https://web.archive.org/web/20170225044124/https://geofeedia.com/products/geolocation-social-media-monitoring/ [https://perma.cc/AG83-6YJF]; Joshua Hall, *Geofeedia Expands Its Role in Pioneering Location-Based Intelligence*, TECHPOINT (Apr. 11, 2016), http://techpoint.org/2016/04/geofeedia-expands-its-role-in-pioneering-location-based-intelligence/ [https://perma.cc/9ZJY-GJ5H].

17. *See* GEOFEEDIA, CASE STUDY: BALTIMORE COUNTY PD, https://www.aclunc.org/docs/20161011_geofeedia_baltimore_case_study.pdf [https://perma.cc/578H-6TA2]; *Public Sector*, DATAMINR, https://www.dataminr.com/public-sector [https://perma.cc/8YFY-WQT7].

18. David S. Cohen, Deputy Dir., Cent. Intelligence Agency, The CIA of the Future, Remarks at the LaFeber-Silbey Endowment in History Lecture at Cornell University (Sept. 17, 2015), https://www.cia.gov/news-information/speeches-testimony/2015-speeches-testimony/deputy-director-cohen-delivers-remarks-on-cia-of-the-future-at-cornell-university.html [https://perma.cc/EWK8-24HM].

19. The term "going dark" is used in the law enforcement and intelligence context to describe the problem of technological advances in privacy outpacing government capabilities to collect critical information. *See* James B. Comey, Dir., Fed. Bureau of Investigation, Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?, Remarks at the Brookings Institution (Oct. 16, 2014), https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course [https://perma.cc/B6TM-3LEN]. For a more optimistic view, see BERKMAN CTR. FOR INTERNET & SOC'Y, DON'T PANIC: MAKING PROGRESS ON THE "GOING DARK" DEBATE (2016), https://cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf [https://perma.cc/2LKN-2A5W].

III. LEGALITY OF COLLECTING AND ANALYZING PUBLIC COMMUNICATIONS DATA

A. The Fourth Amendment Does Not Protect Public Posts on Social Media

The Fourth Amendment does not bar government collection and analysis of public communications on social media. Nevertheless, as the popularity of such surveillance tools has increased among law enforcement agencies across the country,[20] so too have concerns about privacy and civil liberties.[21] The question of whether government surveillance through social media monitoring is a permissible investigatory technique begins with the Fourth Amendment prohibition against unreasonable searches.[22] The Fourth Amendment does not protect what is knowingly exposed to the public,[23] or voluntarily turned over to third parties.[24] Lower courts have thus held the Fourth Amendment does not protect information posted on a public-facing webpage.[25] Nor does the Fourth Amendment protect the GPS coordinates embedded in the metadata of a public post, even when special software is required to extract the infor-

---

20. Rachel Cohn & Angie Liao, *Mapping Reveals Rising Use of Social Media Monitoring Tools by Cities Nationwide*, BRENNAN CTR. FOR JUST. (Nov. 16, 2016), https://www.brennancenter.org/blog/mapping-reveals-rising-use-social-media-monitoring-tools-cities-nationwide [https://perma.cc/MUM2-2JH3]; *see also* Jan Ransom, *Boston Police Set to Buy Social Media Monitoring Software*, BOS. GLOBE (Nov. 26, 2016), https://www.bostonglobe.com/metro/2016/11/25/boston-police-set-buy-social-media-monitoring-software/Vswk24jmuBkuMmPbPY4iYI/story.html (last visited Dec. 20, 2017).

21. *See, e.g.*, Matt Cagle, *Facebook, Instagram, and Twitter Provided Data Access for a Surveillance Product Marketed to Target Activists of Color*, ACLU N. CAL. (Oct. 11, 2016), https://www.aclunc.org/blog/facebook-instagram-and-twitter-provided-data-access-surveillance-product-marketed-target [https://perma.cc/M52D-2WLA].

22. U.S. CONST. amend. IV.

23. Katz v. United States, 389 U.S. 347, 351–52 (1967) ("What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." (internal citations omitted)).

24. Third-party doctrine holds that a person has no Fourth Amendment protection in the information they voluntarily convey to a third party — that is, another person or private business. *See, e.g.*, United States v. Miller, 425 U.S. 435, 443 (1976) ("[T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed."); *see also* United States v. Carpenter, 819 F.3d 880, 885–90 (6th Cir. 2016) (holding subscriber has no reasonable expectation of privacy in cell-site records maintained by service provider), *cert. granted*, 137 S. Ct. 2211 (2017).

25. *See* United States v. Gines-Perez, 214 F. Supp. 2d 205, 225 (D.P.R. 2002) ("[I]t strikes the Court as obvious that a claim to privacy is unavailable to someone who places information on an indisputably, public medium, such as the Internet, *without taking any measures to protect the information*." (emphasis in original)).

mation.[26] Even when the government compiles and organizes public information in a readily accessible database, such information does not automatically become protected by the Fourth Amendment.[27] There is no Fourth Amendment "search" when the government views what a person makes public.

However, many courts and commentators have theorized how aggregation and analysis of public data might implicate a privacy interest.[28] Under the "Mosaic Theory,"[29] the individual data points of a person that she exposes to the public become protected by the Fourth Amendment in the aggregate, where they may reveal "political and religious beliefs, sexual habits, and so on."[30] While this theory bears relevance to the long-term surveillance of social media posts of an individual, social media companies already perform this function when they neatly package such information on an individual's Facebook wall or Twitter page.[31] The integration of location information with the posts via specialized software may add more tiles to the mosaic, but not in a qualitatively different way than if investigators extracted the location information themselves for each post of interest.[32] And while the Supreme Court may alter the doctrine when it decides *United States v.*

---

26. *See* United States v. Post, 997 F. Supp. 2d 602, 605 (S.D. Tex. 2014) (holding Fourth Amendment does not protect GPS metadata of an image uploaded to a website for third parties to view).

27. *See* State v. Sloane, 939 A.2d 796, 803 (N.J. 2008) (ruling a query of the National Crime Information Center database is not a Fourth Amendment search because the records in the database are public).

28. *See* United States v. Jones, 565 U.S. 400, 416–17 (2012) (Sotomayor, J., concurring) (asserting that long-term surveillance of public movements implicates privacy interest); *id.* at 430 (Alito, J., concurring in the judgment) (asserting the same); K.A. Taipale, *Data Mining and Domestic Security: Connecting the Dots to Make Sense of Data*, 5 COLUM. SCI. & TECH. L. REV. 1 (2003) (arguing privacy value of "practical obscurity" is negated by integrating previously disperse information); Emily Berman, *When Database Queries Are Fourth Amendment Searches* 4–5, 12–17 (Aug. 7, 2017) (unpublished manuscript), https://ssrn.com/abstract=2902635 [https://perma.cc/F2T2-MGHP] (arguing Fourth Amendment "search" occurs when government analyzes aggregated data to obtain private information that otherwise could only be known by getting a warrant). *But see* United States v. Carpenter, 819 F.3d at 888–89 (distinguishing *Jones*, where government installed tracking device, from a case where government obtains cell-site location information (CSLI) records maintained by third party), *cert. granted*, 137 S. Ct. 2211 (2017).

29. *See generally* Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311 (2012).

30. *Jones*, 565 U.S. at 416 (Sotomayor, J., concurring).

31. *See, e.g.*, Donald Trump (@realDonaldTrump), TWITTER, https://twitter.com/realDonaldTrump [https://perma.cc/NN8K-7YBV].

32. For posts with geolocation information embedded in the metadata, the information can be accessed through a series of simple steps with publicly available software. *See* Aseem Kishore, *How to Determine Where a Photo Was Taken*, ONLINE TECH TIPS (Aug. 13, 2012), http://www.online-tech-tips.com/computer-tips/how-to-determine-where-a-picture-was-taken/ [https://perma.cc/582S-MKR2]; Kate Murphy, *Web Photos That Reveal Secrets, Like Where You Live*, N.Y. TIMES (Aug. 11, 2010), http://www.nytimes.com/2010/08/12/technology/personaltech/12basics.html (last visited Dec. 20, 2017).

Carpenter,[33] adopting the Mosaic Theory would be a significant alteration of the current legal doctrine.[34] Moreover, the holding would need to be extended beyond protecting information in the hands of third parties to include information made public. Until then, if a user desires Fourth Amendment protection in the privacy of his social media posts, he shouldn't make them public.[35]

B. First Amendment Rights Are Not Infringed by Government Surveillance of Public Social Media Posts

The knowledge that a government official may view or analyze a public communication may cause the user to exercise discretion when it comes to posting sensitive information, even without social media surveillance software. Yet, while the "awareness that the Government may be watching chills associational and expressive freedoms,"[36] the government is not required to turn a blind eye to what is in plain view.[37] The courts have consistently rejected First Amendment claims that associational and expressive freedoms are violated by good-faith investigative techniques that comply with the Fourth Amendment.[38] Furthermore, a "subjective chill" based on mere existence of a government surveillance

---

33. *See Carpenter*, 819 F.3d at 893 n.24. Lower courts and observers see *Carpenter* as a potential opportunity for the Supreme Court to change the law. *See, e.g.*, United States v. Thompson, 866 F.3d 1149, 1159–60 (10th Cir. 2017) ("At this point, however, we can only speculate how the Supreme Court will address these concerns, now that it has taken up the question of historical CSLI . . . . our analysis of the narrow issue of historical CSLI is governed by the third-party doctrine as it currently exists."); Orin Kerr, *Supreme Court Agrees to Hear 'Carpenter v. United States,' the Fourth Amendment Historical Cell-Site Case*, WASH. POST: VOLOKH CONSPIRACY (June 5, 2017), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2017/06/05/supreme-court-agrees-to-hear-carpenter-v-united-states-the-fourth-amendment-historical-cell-site-case/ (last visited Dec. 20, 2017) (suggesting the adoption of Mosaic Theory may be among the issues decided in the case).

34. *See* Kerr, *supra* note 29, at 328–43 (observing the numerous practical difficulties that such a doctrine, if adopted, would present for law enforcement and the judiciary in its implementation).

35. At the very least, users can change their privacy settings to disable location services. *See, e.g.*, *Facebook and Location*, FACEBOOK HELP CTR., https://www.facebook.com/help/337244676357509 [https://perma.cc/XZQ8-WYGP].

36. United States v. Jones, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring).

37. *See* Illinois v. Andreas, 463 U.S. 765, 771 (1983) ("The plain view doctrine is grounded on the proposition that once police are lawfully in a position to observe an item first-hand, its owner's privacy interest in that item is lost; the owner may retain the incidents of title and possession but not privacy."); United States v. Williams, 592 F.3d 511, 521–22 (4th Cir. 2010) (applying plain view doctrine to search of digital media).

38. Reporters Comm. for Freedom of the Press v. Am. Tel. & Tel. Co., 593 F.2d 1030, 1058–59 (D.C. Cir. 1978) ("The mere prospect that such investigation may occur or, indeed, the actual conduct of such investigation does not 'chill' or otherwise abridge First Amendment rights, even though it may give rise to subjective inhibitions for those who desire to avoid the prospect of investigation altogether."); *see also* Hoffa v. United States, 385 U.S. 293 (1966); Lewis v. United States, 385 U.S. 206 (1966); Lopez v. United States, 373 U.S. 427 (1963).

program is insufficient to claim a violation of First Amendment rights under current doctrine.[39] And given the ability of the government to obtain the same information without specialized software, any additional "chilling effect" based on geospatial or other advanced searches is marginal at best; users already assume the risk that the police or an intelligence agency will view their public posts and associated data, regardless of the software involved. Furthermore, law enforcement and intelligence agencies are prohibited from targeting investigations on the sole basis of activity protected by the First Amendment.[40] Even accepting that abuses have occurred,[41] it is unclear how API-based surveillance software adds serious additional risk of infringing on First Amendment rights; traditional application-layer searches can target users based on hashtags and keywords, whereas API-based software only adds content-neutral geographic and temporal parameters.

IV. ADVERSARIALISM BY SURVEILLANCE INTERMEDIARIES

A. Increasing Adversarialism

Social media, technology, and telecommunications companies serve as intermediaries between private citizens and the government.[42] Perhaps viewing the absence of constitutional or other legal protections as an opportunity to capitalize on unmet demand for additional privacy safeguards, many of these intermediaries have taken increasingly adversarial postures toward government surveillance.[43] Apple's highly public

---

39. Clapper v. Amnesty Int'l USA, 568 U.S. 398, 401 (2013) (holding that objectively reasonable likelihood of surveillance under Section 702 of the Foreign Intelligence Surveillance Act was insufficient basis for First Amendment claim); Laird v. Tatum, 408 U.S. 1, 10–15 (1972) (holding that subjective chill based on mere existence of Army's data-gathering system was insufficient basis for First Amendment claim).

40. *See* FED. BUREAU OF INVESTIGATION, DOMESTIC INVESTIGATIONS & OPERATIONS GUIDE § 4.2 (2013), https://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29/fbi-domestic-investigations-and-operations-guide-diog-2013-version/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29%202013%20Version%20Part%2001%20of%2001/view [https://perma.cc/4FMF-EEVT].

41. Despite strict policies prohibiting investigative techniques that target groups based solely on conduct protected by the First Amendment, unconstitutional surveillance is not a new problem. *See, e.g.*, David J. Garrow, *The FBI and Martin Luther King*, THE ATLANTIC (July/Aug. 2002), https://www.theatlantic.com/magazine/archive/2002/07/the-fbi-and-martin-luther-king/302537/ [https://perma.cc/E2M7-QXBB]. Even in the context of social media surveillance software, there are allegations of abuse. *See, e.g.*, Kimberly McCullough, *#BlackLivesMatter Tracked by Oregon DOJ With Social Media Monitoring Software*, ACLU OR. (May 4, 2016), http://www.aclu-or.org/blog/blacklivesmatter-tracked-oregon-doj-social-media-monitoring-software [https://perma.cc/3MJH-HA8Y].

42. *See generally* Alan Z. Rozenshtein, *Surveillance Intermediaries*, 70 STAN. L. REV. (forthcoming 2018), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2935321 [https://perma.cc/V5Z4-84FA].

43. *Id.* (manuscript at 20).

and controversial litigation against a court order compelling assistance to break into a locked iPhone stands as the prime example of this trend.[44] Unsurprisingly, this type of adversarial posturing has spilled over from the encryption showdown and "going dark" debate[45] into the field of social media monitoring software.

In response to public outcry about social media monitoring software,[46] popular social networks have recently begun restricting access to developers who make special software for surveillance. For example, in May 2016, Twitter cut off intelligence agencies' access to the intelligence product of Dataminr, an API-based application which runs sophisticated algorithms to identify unfolding terrorist threats and civil unrest.[47] More recently, on March 13, 2017, Facebook changed its developer policy to prohibit developers from using its API to create software used for surveillance.[48] Facebook's policy is similar to Twitter's developer agreement, which provides:

> Twitter Content . . . may not be used by, or knowingly displayed, distributed, or otherwise made available to . . . any entity for the purposes of conducting or providing surveillance . . . in a manner that would be inconsistent with out users' reasonable expectations of privacy . . .[49]

Twitter references their users' "reasonable expectations of privacy" — invoking the *Katz* standard[50] — inaccurately using legal language to describe a policy decision that itself is at odds with legal doctrine.[51]

---

44. *Id.* (manuscript at 20–23) (discussing Apple's high-profile litigation against DOJ requests for technical assistance).

45. *See* Comey, *supra* note 19.

46. *See, e.g.*, Chris Moody, *Developer Policies to Protect People's Voices on Twitter*, TWITTER DEVELOPER BLOG (Nov. 22, 2016), https://blog.twitter.com/developer/en_us/topics/community/2016/developer-policies-to-protect-peoples- voices-on-twitter.html [https://perma.cc/F8DG-Q3HV] ("Recent reports about Twitter data being used for surveillance, however, have caused us great concern."); Facebook U.S. Public Policy, FACEBOOK (Mar. 13, 2017), https://www.facebook.com/uspublicpolicy/posts/1617594498258356 [https://perma.cc/GWQ9-22A6] (observing role of ACLU in policy change).

47. Christopher S. Stuart & Mark Maremont, *Twitter Bars Intelligence Agencies from Using Analytics Service*, WALL ST. J. (May 8, 2016), https://www.wsj.com/articles/twitter-bars-intelligence-agencies-from-using-analytics-service-1462751682 (last visited Dec. 20, 2017).

48. *Facebook Platform Policy*, FACEBOOK FOR DEVELOPERS, https://developers.facebook.com/policy/ [https://perma.cc/YRW9-4RM7] (banning use of "data obtained from us to provide tools that are used for surveillance").

49. *Developer Agreement & Policy*, TWITTER, https://dev.twitter.com/overview/terms/agreement-and-policy [https://perma.cc/AK9X-J9YA].

50. Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring).

51. Given the meaning of "reasonable expectations of privacy" as a term of art in current Fourth Amendment doctrine, there is no denying the irony of liberally sharing user data with

Through use restrictions on APIs, social media companies seek to protect what the Fourth Amendment does not.

Restrictions like these, to the extent they are enforced,[52] can effectively prohibit rapid intelligence gathering and analysis by law enforcement agencies, while still affording commercial entities the advantages of API-based predictive analytics and alerts.[53] Without the ability to build special surveillance software using APIs, law enforcement agencies, like the average user, can only access social media data at its application layer. One engineer considered how the government would go about collecting intelligence in the absence of a tool, like Geofeedia, built from Twitter's API:

> Even with a warehouse full of people reading tweets, if you wanted a geospatial view, you'd have to train those folks on the kabuki of clicks to get to expose the metadata with the GPS info (if available). So for each tweet in the world, you'd have to click through, find the location, if it was the wrong location throw it away, if it was the right location go back and read the content. Impossible to do at scale.[54]

Thus, while Twitter and Facebook continue to permit the use of its API for any other purposes, law enforcement is deprived of the practical capability to analyze public posts en mass.

In contrast to the voluntary cooperation seen in the years immediately following 9/11,[55] today's surveillance intermediaries generally do not hand over data unless the government utilizes formal legal processes to compel its production.[56] There is every reason to believe this trend will continue under the Trump Administration, which has already been suspected of abusing surveillance authorities for political reasons.[57] Yet, the

---

other private parties while denying access to the government for arguably more important purposes. *See supra* text accompanying note 23.

52. Privacy groups are skeptical about the diligent monitoring and enforcement of these policies. *See, e.g.*, Lily Hay Newman, *Facebook's Big 'First Step' to Crack Down on Surveillance*, WIRED (Mar. 17, 2017), https://www.wired.com/2017/03/facebooks-big-first-step-crack-surveillance [https://perma.cc/L3TS-58EV]; *see also infra* Part IV.

53. *See* Stuart & Maremont, *supra* note 47; *see also* Bala Iyer & Mohan Subramaniam, *The Strategic Value of APIs*, HARV. BUS. REV. (Jan. 7, 2015), https://hbr.org/2015/01/the-strategic-value-of-apis [https://perma.cc/7DK8-R82T].

54. Email from Dr. Jana L. Schwartz, Ph.D., Draper Laboratory (Apr. 7, 2017, 09:41 EST) (on file with author).

55. *See generally* Jon D. Michaels, *All the President's Spies: Private-Public Intelligence Partnerships in the War on Terror*, 96 CALIF. L. REV. 901, 908–21 (2008).

56. *See* Rozenshtein, *supra* note 42, at 18.

57. *See, e.g.*, Twitter Inc. v. Dep't of Homeland Sec., No. 3:17-cv-01916 (N.D. Cal. filed Apr. 6, 2017) (seeking declaratory and injunctive relief from complying with subpoena that requests account information of the user "@ALT_USCIS" who has been critical of the Administration's policies); Mike Isaac, *U.S. Blinks in Clash With Twitter; Drops Order to Unmask*

@ALT_USCIS and DistruptJ20.org lawsuits demonstrate the effectiveness of existing legal mechanisms in protecting against politically motivated violations of privacy: Twitter and DreamHost successfully challenged government attempts to access personally-identifying information about political dissidents. While the potential for politically motivated surveillance is a serious concern, API-based social media surveillance tools do not circumvent the role of technology companies in guarding IP addresses from illegal or overly broad government requests; a subpoena,[58] search warrant,[59] or national security letter[60] is still required for the government to access private account-holder information.

B. Problems of Twitter's and Facebook's Developer Policies

While cooperative arrangements between the government and social media companies have not perished completely,[61] the scale and scope of the arrangements are entirely at the discretion of the private companies. As recently observed in a proposal for regulating social media companies' counter-terrorism programs, private companies are not the proper parties to make determinations about national security issues.[62] And, on

---

Anti-Trump Account, N.Y. TIMES (Apr. 7, 2017), https://www.nytimes.com/2017/04/07/technology/us-blinks-in-clash-with-twitter-drops-order-to-unmask-anti-trump-account.html (last visited Dec. 20, 2017) (reporting Department of Homeland Security's withdrawal of subpoena); *see also* United States's Motion for DreamHost to Show Cause, *In re* Search of www.disruptj20.org that is Stored at Premises Owned, Maintained, Controlled, or Operated by DreamHost, No. 2017-CSW-003438 (D.C. Super. Ct. 2017) (seeking to compel host of anti-Trump website to turn over IP addresses of visitors to site in connection with prosecution of inauguration day protestors); Non-Party DreamHost, LLC's Response in Opposition to United States' Motion for DreamHost to Show Cause, *In re* Search of www.disruptj20.org that is Stored at Premises Owned, Maintained, Controlled, or Operated by DreamHost, No. 2017-CSW-003438 (D.C. Super. Ct. 2017) (observing 1.3 million IP addresses fall within scope of search warrant); Government's Reply in Support of its Motion to Show Cause, and Motion to Modify Attachment B of the Search Warrant, *In re* Search of www.disruptj20.org that is Stored at Premises Owned, Maintained, Controlled, or Operated by DreamHost, No. 2017-CSW-003438 (D.C. Super. Ct. 2017) (narrowing scope of search warrant and explaining original warrant was sought without knowledge of the volume of data requested).

58. *See* 18 U.S.C. § 2703(d) (2012).

59. *See* 18 U.S.C. § 2703(c)(2) (2012).

60. *See* Electronic Communications Privacy Act, 18 U.S.C. § 2709 (2012); Fair Credit Reporting Act, 15 U.S.C. §§ 1681u-1681v (2012); National Security Act of 1947, 50 U.S.C. § 3162 (2012); Right to Financial Privacy Act, 12 U.S.C. § 3414(a)(5) (2012).

61. *See, e.g.*, Joseph Menn, *Social Networks Scan for Sexual Predators, with Uneven Results*, REUTERS (July 12, 2012), http://www.reuters.com/article/us-usa-internet-predators-idUSBRE86B05G20120712 [https://perma.cc/ZX89-6786] (reporting Facebook scans user conversations for profiles of pedophile grooming behavior); Reuters, *Twitter Shuts Down 360,000 Accounts for Links to Terrorism*, NEWSWEEK (Aug. 18, 2016), http://www.newsweek.com/twitter-islamic-state-360000-isis-accounts-terrorism-al-qaeda-491568 [https://perma.cc/3TYV-7NNP] (reporting Twitter shuts down accounts used by ISIS for recruiting).

62. Susan Klein & Crystal Flinn, *Social Media Compliance Programs and the War Against Terrorism*, 8 HARV. NAT'L SEC. J. 53, 70–73 (2017) (arguing private companies are not the

a less philosophical point, the method chosen by social media companies to address problems like terrorism not only could fail to be effective but also undermine the government's broader strategy.[63] The recent changes to developer policies demonstrate exactly the kind of unilateral decision that may undermine government national security and law enforcement strategy. Thus, social media companies should reverse recent changes to their policies that restrict access to APIs based on knowledge of a surveillance purpose, or decline to enforce policies that have already been changed.

The ability to enforce these policies and the wisdom of doing so are both questionable. Criminal enforcement against fourth-party developers who might violate the developer policy is unavailable —the Computer Fraud and Abuse Act[64] ("CFAA") does not criminalize the violation of use restrictions stated in terms of service.[65] Even if the CFAA provided social media companies a basis for civil enforcement,[66] these specific API developer policies remain problematic.

The term "surveillance" is ambiguous, and could easily be broadly interpreted to cover corporate monitoring of their brand, cybersecurity measures to detect phishing scams, commercial profiling for targeted advertising, or even a simple display feed of an event's hashtag. Dual-use products like Twitterfall,[67] which anyone with a Twitter account — including an intelligence analyst or detective — can use, would become even more common tools for surveillance. Ironically, this predictable result would effectively undermine the privacy interests that social media companies claim to champion; without the ability to narrowly refine searches based on advanced algorithms, more innocent users would be swept up in broader queries while terrorists and criminals benefit from greater practical obscurity.

Additionally, the "knowingly" standard simultaneously overburdens developers who unknowingly created dual-use applications while re-

---

correct parties to rely on for "evaluating what constitutes legally impermissible terror-related online activity").

63. For example, social media companies that shut down accounts they determine to be related to terrorist activity can be ineffective, as users can simply create new accounts or move to another platform, and counterproductive, as shutting down accounts can inhibit the government's investigative strategies that seek to exploit the intelligence value of known terrorists' online profiles and their networks. *See, e.g.*, *id.*

64. 18 U.S.C. § 1030 (2012).

65. Though this is a developing area of law, the Ninth Circuit has established some well-reasoned precedents. *See* United States v. Nosal, 676 F.3d 854, 863 (9th Cir. 2012) (holding the phrase "exceeds authorized access" in the CFAA does not extend to violations of use restrictions). *Cf.* Facebook, Inc. v. Power Ventures, Inc., 844 F.3d 1058, 1067 (9th Cir. 2016) ("[A] violation of the terms of use of a website — without more — cannot establish liability under the CFAA.").

66. *Cf.* EF Cultural Travel BV v. Zefer Corp., 318 F.3d 58, 62 (1st Cir. 2003) (affirming grant of preliminary injunction against the use of a scraper bot in violation of CFAA, stating an explicit statement on the website restricting access could establish lack of authorization).

67. *See, e.g.*, TWITTERFALL, https://twitterfall.com (last visited Dec. 20, 2017).

maining toothless in restricting developers who recklessly or negligently provided a surveillance platform. The standard implies that once a developer has notice his application is being used for surveillance, the developer necessarily stands in violation of the policy. This standard imposes unfair consequences on those developers whose applications may be used for surveillance, contrary to their intent. Ironically, Twitter and Facebook, who surely know their public-facing websites are also used for investigatory purposes,[68] would be the parties enforcing their terms against similarly situated developers. Even if social media companies were to selectively enforce only against developers who make products intentionally for law enforcement and intelligence agencies, developers could still easily violate the company's policy without any consequence by claiming their software should be considered dual-use. Furthermore, unless the developers have an affirmative duty to inquire and monitor every use of their software, it is possible that some developers may recklessly or negligently provide a surveillance platform while remaining in compliance with the agreement.

Enforcing these policies could also encourage developers to circumvent the categorization of their products as surveillance software, similar to the model of circumventing approval by the Food and Drug Administration, whereby pharmaceuticals and devices can be used for unapproved purposes or "off-label use"[69] so long as they are not marketed as such.[70] Such a result would only push government surveillance into the shadows without any concomitant gain in user privacy. Similarly, an intelligence agency might respond by contracting out surveillance to "straw man" companies who can use API-based applications for surveillance without alerting the fourth-party developer as to the true nature of the use.[71] Indeed, if social media companies were to enforce such policies without any resistance, discreet outsourcing of surveillance might be the government's best option available, and may already be occurring in secret.

---

68. *See, e.g.*, Behrman, *supra* text accompanying note 10.

69. *See generally* Buckman Co. v. Plaintiffs' Legal Comm., 531 U.S. 341 (2001).

70. 21 U.S.C.A. § 352 (West 2016) (defining Misbranded drugs and devices); *see also* UNDERSTANDING UNAPPROVED USE OF APPROVED DRUGS "OFF LABEL," U.S. FOOD & DRUG ADMIN., https://www.fda.gov/ForPatients/Other/OffLabel/default.htm [https://perma.cc/96W8-QKAG].

71. "Fourth-party" refers to private software developers who use APIs from third-party social media companies to provide the government (the second party) the ability to surveil the user (the first party).

C. Ensuring API Access for Social Media Surveillance Software

Given the disparate stakeholders and incentives of social media companies,[72] these policy arguments are unlikely to persuade social media companies to reverse course. As Tim Cook did through his letter to consumers with regards to encryption,[73] Facebook and Twitter have crossed the Rubicon with regards to their policies of enabling government surveillance in the absence of legal process. Since reverting back to policies that allow for surveillance is unlikely and current legal processes fail to provide a mechanism for the government to compel API access for fourth-party developers, legislation is required to provide such a mechanism.

As traditional subpoenas, warrants, and other court orders require particularized suspicion[74] — and in this case, it is the fourth-party developers who actually access the API-layer data, rather than the government — current methods of legal compulsion are inadequate and inappropriate for securing continued API access for surveillance software. As a preliminary matter, judicial compulsion might be appropriate for *ex post facto* investigations that seek historical communications within a given geography to identify potential culprits, witnesses, or relevant content. However, much of the intelligence value of social media surveillance software is derived from real-time analyses and monitoring without any particular target.[75] As Professors Niva Elkin-Koren and El-

---

72. *See in re* Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by this Court, 149 F. Supp. 3d 341, 369 (E.D.N.Y. 2016) (observing Apple's argument that rendering technical assistance to the government "could threaten the trust between Apple and its customers and substantially tarnish the Apple brand" (citing Apple's initial memorandum in partial opposition)); Rozenshtein, *supra* note 42, at 26–27 (observing business incentives to signal commitment to user privacy and fight government surveillance requests to receive good marks on the Electronic Frontier Foundation's *Who's Got Your Back* annual report). *But see* Niva Elkin-Koren & Eldar Haber, *Governance by Proxy: Cyber Challenges to Civil Liberties*, 82 BROOK. L. REV. 105, 115–16 (2016) (discussing the alignment of incentives for public-private partnerships and the "invisible handshake" between online intermediaries and government).

73. Apple had intentionally eliminated its ability to unlock such devices for law enforcement with the rollout of its iOS 8 software. In its updated privacy policy, Apple declared it will no longer perform iOS data extractions in response to government search warrants, and that user data is protected by an encryption key tied to the user's passcode, which Apple does not possess. *See Privacy*, APPLE INC., https://www.apple.com/privacy/government-information-requests [https://perma.cc/A6FR-RSRV]; *see also* Cyrus Farivar, *Apple Expands Data Encryption Under iOS 8 Making Handover to Cops Moot*, ARS TECHNICA (Sept. 18, 2014), http://arstechnica.com/apple/2014/09/apple-expands-data-encryption-under-ios-8-making-handover-to-cops-moot [https://perma.cc/9JN6-KPFY] (noting Apple had the ability to provide data on locked devices to law enforcement prior to updated policy).

74. U.S. CONST. amend. IV; FED. R. CRIM. P. 41(e)(2)(A) (requiring warrants to identify the person or property to be searched or seized); 18 U.S.C. § 3123(b)(1) (2012) (requiring specificity in pen register/trap and trace device order); 18 U.S.C. § 2703(d) (2012) (requiring specificity for an order under the Stored Communications Act).

75. *See, e.g.*, *supra* note 16.

dar Haber observe, "the use of big data and social media analytics for monitoring threats, predicting harmful activities, and prevention, require access to bulk data. Consequently, it is no longer sufficient to acquire an individual warrant in order to perform law enforcement tasks."[76] Whereas a judge can review the facts sworn by oath or affidavit and make an informed judgment about whether there is probable cause to search a particular subject for particular things, a judge does not have such facts when evaluating a surveillance program.[77] This critical difference between surveillance and searches calls into question the wisdom of subjecting surveillance programs to judicial scrutiny in Article III courts, since there is no target or suspect at this stage, much less a "case or controversy" or adversarial proceeding.[78] More practically, the requirement of judicial approval for each query on social media surveillance software would make it impossible for police departments to improvise or respond to events in real time.

An alternative approach would be requiring programmatic approval of social media surveillance. Professor Emily Berman suggests that database queries could be subjected to judicial scrutiny, using Section 702 of the Foreign Intelligence Surveillance Act as a model,[79] to ensure privacy is safeguarded notwithstanding the lack of a warrant requirement to collect communications.[80] Law enforcement and intelligence agencies would have to certify to a judge that they have implemented minimization procedures for storing, analyzing, and disseminating sensitive personal information shared publicly on social media. However, if judicial approval of minimization procedures makes it reasonable to programmatically collect private messages,[81] which are normally afforded Fourth

76. Elkin-Koren & Haber, *supra* note 72, at 156.

77. Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757, 803 (1994) (particularity of the warrant requirement of the Fourth Amendment "presuppose[s] a search for items akin to contraband or stolen goods, not 'mere evidence' such as where the target was and when she was there, which video surveillance could establish.").

78. *See* Nola K. Breglio, *Leaving FISA Behind: The Need to Return to Warrantless Foreign Intelligence Surveillance*, 113 YALE L.J. 179, 205–08 (2003) (discussing arguments against judicial authorization of surveillance) (citing TELFORD TAYLOR, TWO STUDIES IN CONSTITUTIONAL INTERPRETATION 79–85 (1969)).

79. *See* Berman, *supra* note 28, at 23; *see also* 50 U.S.C.A. § 1881a (West 2015). *See generally* DAVID S. KRIS & J. DOUGLAS WILSON, NATIONAL SECURITY INVESTIGATIONS AND PROSECUTIONS § 17:9 (2d ed. 2012).

80. *See* NAT'L SEC. AGENCY ET AL., UNITED STATES SIGNALS INTELLIGENCE DIRECTIVE 18: LEGAL COMPLIANCE AND U.S. PERSONS MINIMIZATION PROCEDURES (2011); NAT'L SEC. AGENCY, MINIMIZATION PROCEDURES USED BY THE NSA IN CONNECTION WITH ACQUISITIONS OF FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (2011).

81. *See* United States v. Mohamud, 843 F.3d 420, 443 (9th Cir. 2016) (holding collection under § 702 did not violate Fourth Amendment because targeting and minimization procedures adequately protected diminished privacy interest in communications sent to third party).

Amendment protection,[82] certainly social media surveillance deserves even less judicial scrutiny, where the collection and analysis of public communications implicate no Fourth Amendment rights under current constitutional doctrine.[83]

The All Writs Act is also an unsuitable method of compelling API access.[84] The Act broadly empowers a court to compel a person to render assistance necessary to the court's jurisdiction in accordance with the law.[85] Recently the government has sought All Writs Act orders to compel Apple to render technical assistance to defeat encrypted hardware and access data for which the court had issued a search warrant.[86] However, as discussed above, surveillance using API-enabled software is different from a search warrant for particular information. Because social media surveillance software does not access data through the exercise of a court's jurisdiction — in other words issuing a search warrant or court order — the All Writs Act is of no avail in securing API access. Rather, since obtaining API access relates to a manner of providing information, rather than enforcing a judicially determined right to previously unavailable information, a different statutory authority is warranted.

V. A PROPOSAL FOR EQUAL ACCESS TO PUBLIC COMMUNICATIONS DATA

A. Equal Access to Public Communications Act

The most appropriate means of securing API access for social media surveillance software is a narrowly circumscribed legislative amendment to the Communications Assistance to Law Enforcement Act ("CALEA").[87] The purpose of such a proposal, hereinafter referred to as the Equal Access to Public Communications Act ("EAPCA"), is to ensure that the social media companies that make their APIs freely available to software developers cannot deny law enforcement and intelligence

82. *See* United States v. Warshak, 631 F.3d 266, 285–86 (6th Cir. 2010) (holding that contents of emails carry same reasonable expectation of privacy as letters in sealed envelopes).

83. *See supra* Part II.

84. *See* 28 U.S.C. § 1651(a) (2012).

85. *See id.*; *see also* United States v. N.Y. Tel. Co., 434 U.S. 159, 174 (1977) (holding court order compelling respondent telephone company, though not party to the original action or engaged in wrongdoing, to provide assistance to an FBI investigation was authorized by the Act).

86. *See in re* Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by this Court, 149 F. Supp. 3d 341, 354 (E.D.N.Y. 2016) (denying government's application under All Writs Act for order to bypass Apple device passcode security); *in re* Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, Ca. License Plate 35KGD203, No. ED 15-0451M, 2016 WL 618401, at *1 (C.D. Cal. Feb. 16, 2016) (ordering Apple to assist agents in search of a smartphone).

87. *See* 47 U.S.C. §§ 1001–10 (2012).

agencies the capability to lawfully collect and analyze publicly available information. The EAPCA would effectively prevent social media companies from discriminating against lawful government end-use in its API developer policies.

CALEA provides a logical entry point for integrating this statutory authority because of its historical purpose in ensuring that technological developments do not effectively prevent lawful government surveillance.[88] CALEA requires telecommunications companies to comply with legal process by making lawfully sought information available in a manner that is readily understood.[89] This proposed EAPCA could be construed as a "social media company assistance to law enforcement (and intelligence agencies)" equivalent, in that it mandates a format for otherwise legally available data, rather than legislating new authority to collect previously unavailable information. Unlike CALEA, however, in this case, the companies need not build the surveillance-friendly application themselves, nor even release API access directly to the government. Rather, they may comply by returning access to fourth-party developers.

The Stored Communications Act ("SCA") could also provide an appropriate statutory home for the EAPCA. Where the SCA already has a section titled "Required disclosure of customer communications or records,"[90] the EAPCA would follow as "Required access to public communications or records." Unlike the various procedures for compelling disclosure of different types of stored communications and records under the SCA,[91] the EAPCA would simply require that social media companies that make their APIs publicly available for software development shall not prohibit use or otherwise restrict access to a developer on the sole basis that the product serves a purpose associated with lawful investigatory or intelligence-gathering activity. In addition, the EAPCA would also provide that an intended or knowing use associated with lawful investigatory or intelligence-gathering activity shall be an affirmative defense for a developer in any civil action for breach of developer agreement.

Undoubtedly, this amendment would invite litigation and possibly a legislative response at the state level. Nevertheless, the current legal doctrines under the First and Fourth Amendments allow for the collection, aggregation, and analyses of public communications.[92] And of course, like any statute, definitional issues abound: for example, the

88. *See* H.R. REP. NO. 103-827(I), at 9 (1994), *as reprinted in* 1994 U.S.C.C.A.N. 3489 ("The purpose of . . . [CALEA] is to preserve the government's ability, pursuant to court order or other lawful authorization, to intercept communications involving advanced technologies such as digital or wireless transmission modes . . . while protecting the privacy of communications and without impeding the introduction of new technologies, features, and services.").

89. *See* 47 U.S.C. § 1002(a) (2012).

90. 18 U.S.C.A. § 2703 (West 2016).

91. *See* 18 U.S.C.A. § 2703(d) (West 2016).

92. *See supra* Part II.

question of which entities qualify as a "social media company" or whatever equivalent terminology is chosen through the legislative process. Such issues would need to be resolved in the drafting process with an eye toward preventing subsequent disqualifying behavior by the targeted companies.

B. Anticipating Opposition to the Proposal

Preventing loopholes in the language of the legislation is relatively straightforward compared to the other potential technical and legal challenges that social media companies may consider as a response. This proposal does *not* directly compel access to the API tools, though the availability of this relatively extreme option portrays the proposed mechanism as modest and reasonable. Rather, by insisting upon equal access to API tools, this proposal confronts social media companies with a tradeoff: either end discrimination against lawful government purposes or end the business model of making APIs freely available to developers.

The former is what this proposal aims to establish since the costs to social media companies are relatively minor, except for some brand tarnishing that would apply to all social media companies and result in little, if any, competitive disadvantage. The risk of massive abandonment of popular social media networks like Twitter, Facebook, and Instagram is negligible due to the power of network effects.[93] Indeed, users of major popular social media companies have the ability to use MySpace and Mastodon already, yet users are not flocking there in droves. While it is possible in theory that users abandon platforms like Facebook with strong network effects,[94] Facebook has shown itself to be a social media Goliath that can withstand a few privacy scandals of its own.[95] In light of the network effects of social media companies, especially for Twitter and Facebook, the suggestion that a modest proposal that returns API access to a status quo of 2016 is hardly scandalous enough to have any meaningful impact on user retention and engagement for the major social network companies.

---

93. *See* Patrick George, *The Scary Truth About Corporate Survival*, HARV. BUS. REV. (Dec. 2016), https://hbr.org/2016/12/the-scary-truth-about-corporate-survival [https://perma.cc/SGH5-XLP8] (explaining how Facebook's one billion users create a competitive advantage because moving to a rival platform would require a steep switching cost of reconnecting with friends and recreating content).

94. Matt Buchanon, *Network Effects and Global Domination: The Facebook Strategy*, WIRED (May 17, 2012), https://www.wired.com/2012/05/network-effects-and-global-domination-the-facebook-strategy **[**https://perma.cc/V4BX-4YFM**].**

95. *See, e.g.*, Vindu Goel, *Facebook Tinkers with Users' Emotions in News Feed Experiment, Stirring Outcry*, N.Y. TIMES (June 29, 2014), https://www.nytimes.com/2014/06/30/technology/facebook-tinkers-with-users-emotions-in-news-feed-experiment-stirring-outcry.html (last visited Dec. 20, 2017).

The latter alternative — the companies' wholesale elimination of APIs — might be considered social media companies' "nuclear option," since it would effectively render the proposed legislation useless. However, this approach would be devastating to the social utility and profitability of the respective companies. Such a response might change the companies' business models to restricting API use based on *ex ante* approval, akin to a highly scrutinized licensing agreement. The costs of hiring the staff to make this option possible, and to review applications for API access quickly, is probably not a significant deterrent. However, aside from going against the Silicon Valley spirit of technological innovation and information sharing, this approach has significant competitive disadvantages. Allowing developers free access immensely benefits social media companies by allowing them to expand into new markets and integrate with complementary services in innovative, unanticipated ways.[96] These benefits improve brand loyalty and awareness, which drive user growth, retention, and engagement.[97] In turn, these critical metrics for social media companies make them more attractive to advertisers and more profitable to investors.[98]

Thus, this proposal is a calculated wager that most social media companies will view the nuclear option as ultimately against their own interests. Nevertheless, these companies may still raise legal challenges to the legislation. While Part III of this Note explains how government surveillance of public social media posts is securely grounded in current legal doctrine, this proposal represents an expansion of the current law, in which the government has no pre-existing right to social media companies' proprietary data. Legal challenges to the proposal would be expected.

Social media companies may take up Apple's argument from its litigation against the Department of Justice last year, that code is a protected form of speech under the First Amendment.[99] Yet, where Apple had a

---

96. *See, e.g.*, Iyer & Subramaniam, *supra* note 53 (describing how Google Maps' popularity skyrocketed after a third-party application showed real estate locations on the map and how Google now has expanded API-based access to its other products as well).

97. *See Business Models for APIs*, IBM (Apr. 26, 2014), https://developer.ibm.com/apiconnect/documentation/api-101/business-models-apis [https://perma.cc/WA98-3UC2] (noting that popular social networks commonly have "[f]ree APIs [that] can drive adoption of APIs and brand loyalty as well as allow the API provider to enter new channels").

98. *See, e.g.*, Reuters, *Facebook Now Has an Almost Advertising-Only Business Model*, FORTUNE (May 5, 2017), http://fortune.com/2017/05/05/facebook-digital-advertising-business-model [https://perma.cc/M4BT-MVN9]; Samantha Masunaga, *Twitter Says Daily Users Grew 14%, and Stock Jumps — Even Though Revenue is Down*, L.A. TIMES (Apr. 26, 2017), http://www.latimes.com/business/technology/la-fi-tn-twitter-earnings-20170426-story.html [https://perma.cc/KYP6-T39Q].

99. *See* Apple Inc.'s Motion to Vacate Order Compelling Apple Inc. to Assist Agents in Search, and Opposition to Government's Motion to Compel Assistance, *In re* Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203, No. 5:16-cm-00010 (C.D. Cal., Feb. 25, 2016).

strong argument against being compelled to write new code — "GovOS"[100] — social media companies would not be required to write a "GovAPI" under this proposal. Rather, social media companies would only have to allow the APIs already available to developers to be used for lawful government surveillance purposes.

Another potential argument would be that the use of social media company's APIs for a purpose it disagrees with would violate its First Amendment freedom of expressive association. However, under *Rumsfeld v. Forum for Acad. and Institutional Rights, Inc.*[101] (hereinafter *FAIR*) such a claim of compelled expressive association must fail. In *FAIR*, the Supreme Court found that schools' decisions on which recruiters can access campus are "not inherently expressive."[102] The Court went on to hold that legislation mandating equal access for military recruiters did not "interfere with any message of the school," as to violate the First Amendment.[103] Similarly, legislation mandating equal access to the public communications data for lawful government activities would not infringe on protected speech or otherwise burden social media companies.

VI. CONCLUSION

To date, there have been no congressional hearings or reports in the press that prove social media surveillance software was critical to stopping a terrorist attack or bringing a suspected criminal to justice.[104] Lacking specific insights into sensitive government records, this Note emphasizes the importance of API-enabled social media surveillance to the ability of law enforcement and intelligence agencies to process vast amounts of public communications data to respond to developments in real time.

Third-party intermediaries can play an important role in safeguarding their users' civil liberties against politically motivated or otherwise illegal conduct by government officials, especially in a political climate

---

100. A shorthand for "government operating system" as a pun of Apple's iOS. *See, e.g.*, Tony Romm, *Apple Launches Court Defense in iPhone Case*, POLITICO (Feb. 25, 2016), http://www.politico.com/story/2016/02/apple-iphone-fbi-219790 [https://perma.cc/U7FN-Y5E7].

101. 547 U.S. 47 (2006) (upholding the Solomon Amendment, requiring schools that accept federal funding to provide the same level of access to campus for military recruiters as they provide to non-military recruiters).

102. *Id.* at 64.

103. *Id.*

104. Such examples are highly persuasive to legislators considering controversial surveillance programs. *See, e.g.*, PRIVACY & CIVIL LIBERTIES OVERSIGHT BD., REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT 109–10 (2014) (citing approximately thirty cases where "Section 702 information was the initial catalyst that identified previously unknown terrorist operatives and/or plots" and concluding that surveillance program was effective).

rife with distrust of government and extreme polarization. In the context of social media surveillance software, however, such concerns are overstated; warrantless surveillance of public social media posts is permissible under current Fourth Amendment doctrine, and the marginal effects on civil liberties caused specifically by API-enabled collecting and processing of public communications data are minimal. Nevertheless, the increasingly adversarial relationship between the government and social media companies suggests that recent changes to API developer policies are unlikely to be reversed without a new legal authority. This Note proposes the creation of new authority by which fourth-party developers who create surveillance software for the government are guaranteed the same access to public communications data as other commercial developers, such that social media companies' business incentives align with law enforcement and intelligence agencies' interest in protecting the public from harm.