IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

DOC SOCIETY and INTERNATIONAL DOCUMENTARY ASSOCIATION, Plaintiffs, v. MICHAEL R. POMPEO, in his official capacity as Secretary of State; and CHAD F. WOLF, in his official capacity as Acting Secretary of Homeland Security, Defendants.	Case No. 1:19-cv-03632-TJK

BRIEF OF *AMICUS CURIAE* ELECTRONIC FRONTIER FOUNDATION IN SUPPORT OF PLAINTIFFS' OPPOSITION TO DEFENDANTS' MOTION TO DISMISS

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page

Cases

Other Authorities

INTERESTS OF AMICUS CURIAE[1]

The Electronic Frontier Foundation (EFF) is a member-supported, nonprofit civil liberties organization that has worked for 30 years to protect free speech, privacy, security, and innovation in the digital world. EFF, with over 30,000 members, represents the interests of technology users in court cases and broader policy debates surrounding the application of law to the Internet and other technologies.

[1] No counsel for a party authored this brief in whole or in part, and no counsel or party made a monetary contribution intended to fund the preparation or submission of this brief. No person other than the *amicus curiae* or their counsel made a monetary contribution intended to fund the brief's preparation or submission. All parties consent to *amicus* filing of this brief.

INTRODUCTION

In the social media age, secrecy should not be a prerequisite for privacy. *See U.S. v. Jones*, 565 U.S. 400, 418 (2012) (Sotomayor, J., concurring). Fifty percent of the world's population uses social media—meaning 3.8 billion people.[2] Seventy-two percent of American adults use social media.[3] Defendants' social media surveillance program, enabled by the Registration Requirement,[4] targets the publicly available information on social media profiles of visa applicants. Yet publicly available content, particularly when viewed comprehensively, can reveal vast amounts of personal details about social media users. "Social media allows users to gain access to information and communicate with one another about it on any subject that might come to mind." *Packingham v. North Carolina,* 137 S. Ct. 1730, 1737 (2017).

Due to the networked nature of social media, personal information about a user may not be published by the user themselves, but rather by their social media connections. Even when a user posts personal information on social media, they may do so inadvertently due to the complexities of privacy settings, within a single platform and across platforms. Moreover, much of this information is outside the scope of and irrelevant to the visa application process, or may not be sufficiently reliable to make a legal determination about visa eligibility.

The networked nature of social media also means that Defendants' social media surveillance program does not solely affect visa applicants, many of whom are already in the

---

[2] Paige Cooper, *140+ Social Media Statistics That Matter to Marketers in 2020*, HOOTSUITE (Feb. 20, 2020), https://blog.hootsuite.com/social-media-statistics-for-social-media-managers.

[3] *Social Media Fact Sheet*, PEW RES. CTR. (June 12, 2019), https://www.pewresearch.org/internet/fact-sheet/social-media.

[4] Visa applicants must "disclose on their application forms all social media identifiers, including pseudonymous ones, they have used on any of twenty social media platforms during the preceding five years (the 'Registration Requirement')." Compl. [ECF No. 1] ¶ 1. Social media identifiers are synonymous with usernames or handles.

United States; it also implicates those in their social networks, many of whom may be U.S. persons. Overall, this amounts to millions, if not billions of people, given that the Registration Requirement will apply to an estimated 14.7 million visa applicants annually.[5]

Thus, social media users have privacy and related free speech interests in shielding their public profiles from government scrutiny. If visa applicants and their social media associates know that the government can glean vast amounts of personal information about them, whether accurate or not, they may be chilled from freely engaging in speech and associational activities on social media platforms like Facebook, Instagram, and Twitter.

Visa applicants may be chilled out of fear that they could be denied a U.S. visa. Visa applicants *and* those in their social networks may be chilled by the simple fact that the U.S. government is, at minimum, *reviewing* vast amounts of personal information about them—such as their political beliefs or sexual orientation, or details about who their friends and family members are, or what groups they belong to. "The characteristics of modern communications technology that enhance association . . . also enhance the potential that association will be chilled by relational surveillance."[6] These chilling effects are heightened by the fact that Defendants may also be *collecting, storing for decades, using for other purposes, and sharing*

---

[5] Compl. [ECF No. 1] ¶ 1; U.S. Dept. of State, *60-Day Notice of Proposed Information Collection: Application for Nonimmigrant Visa*, OMB Control No. 1405-0182 [Forms DS-160 & DS-156] (March 30, 2018) ("Estimated Number of Respondents: 14,000,000."), https://www.federalregister.gov/documents/2018/03/30/2018-06496/60-day-notice-of-proposed-information-collection-application-for-nonimmigrant-visa; U.S. Dept. of State, *60-Day Notice of Proposed Information Collection: Application for Immigrant Visa and Alien Registration*, OMB Control No. 1405-0185 [Form DS-260] (March 30, 2018) ("Estimated Number of Respondents: 710,000."), https://www.federalregister.gov/documents/2018/03/30/2018-06490/60-day-notice-of-proposed-information-collection-application-for-immigrant-visa-and-alien.

[6] Katherine J. Strandburg, *Freedom of Association in a Networked World: First Amendment Regulation of Relational Surveillance*, 49 B.C. L. REV. 741, 751 (2008), https://lawdigitalcommons.bc.edu/bclr/vol49/iss3/3.

with other governmental entities publicly available social media information.[7]

For these reasons, *amicus* urges this Court to deny Defendants' motion to dismiss.

ARGUMENT

I. Government Surveillance of Public Social Media Profiles Invades Privacy and Chills Free Speech and Association

Social media users have privacy and related free speech interests in shielding their profiles from government surveillance, irrespective of the fact that Defendants' Registration Requirement only targets "public-facing" social media information.[8] Defendants can glean vast amounts of personal information from public social media profiles, creating an impermissible chilling effect on both visa applicants and those in their social networks.

A. Defendants' Surveillance Program is Broad in Scope Given the Nature of Social Media

Social media platforms are modern technological innovations that can chronicle in persistent, exhaustive, and minute detail all aspects of individuals' lives. As discussed below, *see infra* Part II, social media profiles can publicly reveal a plethora of personal information about users, both in terms of the amount and nature of that information.

Moreover, Defendants have not meaningfully limited the scope of the social media surveillance program other than by limiting it to publicly available content. While visa applicants have to report social media platforms they have *used* in the past five years, there is no indication that Defendants are limited to only looking at social media content *date stamped* during the five

[7] Compl. [ECF No. 1] ¶¶ 35-37.

[8] U.S. Dept. of State, *DS-160 Supporting Statement*, at 22 (April 11, 2019), https://www.reginfo.gov/public/do/PRAViewDocument?ref_nbr=201808-1405-004; U.S. Dept. of State, *DS-260 Supporting Statement*, (April 10, 2019), https://www.reginfo.gov/public/do/PRAViewDocument?ref_nbr=201808-1405-009.

years prior to the submission of the application.[9]

The Supreme Court has recognized that modern technologies can host unprecedented amounts of data. More than a modern cell phone's "immense storage capacity," *see Riley v. California*, 573 U.S. 373, 393 (2014), social media profiles have virtually unlimited storage capacity because they live in "the cloud"—that is, in companies' ever-expanding server farms.[10] The *Riley* Court noted that "[t]he sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions," *id.* at 394, which may be publicly available on social media platforms like Facebook and Instagram.

Additionally, similar to cell phones, social media profiles "collect[] in one place many distinct types of information … that reveal much more in combination than any isolated record." *See id.* Hundreds or thousands of social media posts, photos and videos, and group memberships can collectively reveal much more about a person than a few discrete pieces of content. Government surveillance of public social media data can thus reveal "a wealth of detail about [their] familial, political, professional, religious, and sexual associations." *See Jones*, 565 U.S. at 415 (Sotomayor, J., concurring). *See also Carpenter v. U.S.*, 138 S. Ct. 2206, 2217 (2018) ("[T]ime-stamped data provides an intimate window into a person's life.").

The government can also glean from social media profiles personal information that it may not otherwise have access to via the visa application. For example, Form DS-260 for

[9] Compl. [ECF No. 1] ¶ 28; *DS-160 Supporting Statement* at 22 & *DS-260 Supporting Statement* at 20, *supra* note 8.

[10] Hive is Facebook's data warehouse, which had (in 2014) 300 petabytes of data and absorbed four new petabytes of data per day. Kit Smith, *53 Incredible Facebook Statistics and Facts*, BRANDWATCH (June 1, 2019), https://www.brandwatch.com/blog/facebook-statistics. Each petabyte is equivalent to one million gigabytes. By comparison, modern smartphones generally hold anywhere from 32 to 128 gigabytes of storage.

immigrant visas rightfully does not ask for political beliefs.[11] Yet political beliefs may be easily ascertainable from a review of a visa applicant's public social media content. *See infra* Part II.A. This is another situation where "the retrospective quality of the data here gives [the government] access to a category of information otherwise unknowable." *See Carpenter*, 138 S. Ct. at 2218.

The breadth of Defendants' social media surveillance program is not just measured by the amount and types of personal information it encompasses. It is also measured by the sheer number of people affected. This includes visa applicants, many of whom are already in the United States, *and* those in their social networks, including U.S. persons.[12]

Defendants admit that the Registration Requirement will affect 14.7 million visa applicants annually.[13] And the social media connections of those visa applicants are many millions—if not billions—more than that.[14] In a striking illustration of the networked nature of social media, Facebook's Cambridge Analytica scandal[15] revealed how directly targeting a small subset of users can invade the privacy of tens of millions of people: "Only 270,000 people ever used the This Is Your Digital Life (TIYDL) app, but Facebook estimates that data from 87

---

[11] *See infra* note 31. *See generally* U.S. Dept. of State, *DS-260 IV Application SAMPLE* (Oct. 2019), https://travel.state.gov/content/dam/visas/DS-260-Exemplar.pdf.

[12] Many visa applicants are already in the country and therefore are themselves U.S. persons. Compl. [ECF No. 1] ¶¶ 1, 43.

[13] *See supra* note 5.

[14] As of 2014, more than half of Facebook users had more than 200 friends. Aaron Smith, *What people like and dislike about Facebook*, PEW RES. CTR. (Feb. 3, 2014), https://www.pewresearch.org/fact-tank/2014/02/03/what-people-like-dislike-about-facebook.

[15] The Cambridge Analytica scandal involved the precise targeting of Facebook users to influence the U.S electorate during the 2016 presidential election. Cambridge Analytica developed a personality quiz and app that scraped private information from the profiles of users who took the quiz, as well as from users' friends' profiles. Kevin Granville, *Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens*, N.Y. TIMES (March 19, 2018), https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html.

million people ended up in the hands of Cambridge Analytica."[16] Even people who choose to avoid social media are not immune from Defendants' social media surveillance program, as data provided to social media platforms by their users can accurately predict the personal information of *nonusers* of social media.[17] *See infra* Part II.A.

Importantly, Defendants have not excluded the possibility of collecting information about visa applicants' social media connections, including U.S. persons.[18]

B. Social Media Users Have Privacy Interests in Their Public Information

Given the broad scope of Defendants' social media surveillance program, visa applicants and those in their social networks have privacy interests in protecting their digital lives from government scrutiny, even when those lives play out in public posts. Although the Fourth Amendment is not at issue in this case, it is noteworthy that the Supreme Court is increasingly recognizing that pervasive government surveillance of individuals' public lives, particularly when facilitated by modern technology, implicates privacy rights. As the Court stated, "[a] person does not surrender all Fourth Amendment protection by venturing into the public sphere." *Carpenter*, 138 S. Ct. at 2217.

---

[16] Timothy Revell, *How Facebook let a friend pass my data to Cambridge Analytica*, NEW SCIENTIST (April 16, 2018), https://www.newscientist.com/article/2166435-how-facebook-let-a-friend-pass-my-data-to-cambridge-analytica. Facebook's own research estimates that there are only 3.57 degrees of separation to connect everyone on the platform. Smriti Bhagat et al., *Three and a Half Degrees of Separation*, FACEBOOK RES. (Feb. 4, 2016), https://research.fb.com/blog/2016/02/three-and-a-half-degrees-of-separation.

[17] David Garcia, *Leaking privacy and shadow profiles in online social networks*, SCIENCE ADVANCES (Aug. 4, 2017), https://advances.sciencemag.org/content/3/8/e1701172.

[18] "With regard to concerns that United States citizen communications may become involved in the collection, the Department limits its collection to information relevant to a visa adjudication. Consular staff will be directed in connection with this collection to take particular care to avoid collection of third-party information *unless relevant and necessary when conducting any review of social media information*." *DS-160 Supporting Statement* at 9 & *DS-260 Supporting Statement* at 8-9 (emphasis added), *supra* note 8.

"[A] central aim of the Framers was to place obstacles in the way of a too permeating police surveillance." *Carpenter*, 138 S. Ct. at 2214 (internal quotation and citation omitted). The Supreme Court has called into question "dragnet-type law enforcement practices" aided by modern technology that encompass individuals' public lives. *Jones*, 565 U.S. at 409 n.6 (citing *U.S. v. Knotts*, 460 U.S. 276, 284 (1983)). *Accord Carpenter*, 138 S. Ct. at 2215 n.2. Importantly, "[a] majority of this Court [in *Jones*] has already recognized that individuals have a reasonable expectation of privacy in the whole of their physical movements," which includes their movements in public. *Carpenter*, 138 S. Ct. at 2217. In *Carpenter*, the Court held that "[w]hether the Government employs its own [GPS] surveillance technology as in *Jones* or leverages the technology of a wireless carrier, … an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through [cell-site location information]." *Id.*

Here, the government is leveraging the technology of social media companies to engage in widespread surveillance of visa applicants and those in their social networks—that is, the government is assisted by the fact that these companies host publicly available, easily retrievable digital records of individuals' personal lives in words, photos, videos, audio recordings, and other data. Social media profiles may reveal not *just* users' physical locations over time, as was at issue in *Jones* and *Carpenter*, but myriad aspects of their personal lives. Moreover, while consular officers will surely manually scroll through public social media content after they obtain visa applicants' account identifiers per the Registration Requirement, the State Department has not stated whether consular officers also plan to use automated tools to increase the efficiency of their comprehensive review. Notably, Defendant U.S. Department of Homeland

Security's (DHS) component agency U.S. Customs and Border Protection (CBP) uses such tools for its own social media surveillance program.[19]

The invasiveness of Defendants' social media surveillance program is compounded by the fact that visa applicants face government review of their social media profiles not only during the visa vetting process, but also after they have arrived in the United States,[20] surely in part because such "long-term monitoring [is] relatively easy and cheap." *See Jones*, 565 U.S. at 429 (Alito, J., concurring in the judgment). Additionally, beyond review, public social media information may also be collected, stored in government databases for upwards of 100 years, used for other purposes, and shared with domestic and foreign governmental entities.[21]

Thus, Defendants' social media surveillance program is another example of why courts should "cease[] [to] treat secrecy as a prerequisite for privacy." *See Jones*, 565 U.S. at 418 (Sotomayor, J., concurring).[22]

This is particularly salient given how social media platforms function. While some social media users knowingly share content publicly, often the public availability of personal

---

[19] "CBP uses Internet-based platforms, as well as government and commercially developed tools that provide a variety of methods for monitoring social media sites." U.S. Customs & Border Protection, *Privacy Impact Assessment for the Publicly Available Social Media Monitoring and Situational Awareness Initiative, DHS/CBP/PIA-058*, at 1 (March 25, 2019), https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp58-socialmedia-march2019.pdf. *See also* Compl. [ECF No. 1] ¶ 57 (discussing the risks of "automated review tools").

[20] Once in the United States, visa applicants (who become visa holders) are subject to ongoing social media monitoring by Defendant DHS's component agencies. Compl. [ECF No. 1] ¶¶ 38, 63. Additionally, visa holders in the U.S. who seek to renew their visas will again be subject to the Registration Requirement. *Id.* ¶ 23.

[21] Compl. [ECF No. 1] ¶¶ 35-37.

[22] It is immaterial that users' social media content is held by technology companies. In *Carpenter* and *Jones,* the Court declined to apply the third-party doctrine. *Carpenter*, 138 S. Ct. at 2216-17; *Jones*, 565 U.S. at 417 (Sotomayor, J., concurring).

information is inadvertent due to the difficulties in navigating the differences in default privacy settings across platforms, the fact that privacy settings may change over time, and the fact that a user's social media connections may reveal information about the user. *See infra* Part II. Even when social media users understand that what they are sharing is public, it is a wholly different situation when the government engages in surveillance of their online accounts to create an "all-encompassing record" of their personal lives. *See Carpenter*, 138 S. Ct. at 2217.

C. Government Surveillance of Public Social Media Information Chills Free Speech and Association

Given that social media users have privacy interests in their public profiles, it follows that government surveillance of their public social media content can chill free speech and association. That is, if individuals know that the government can glean potentially vast amounts of personal information from a comprehensive review of their social media profiles, or that their anonymous or pseudonymous accounts will be linked to their real-world identities, those users will be more inclined to engage in self-censorship and curtail their online speech and associational activities. This risk is particularly constitutionally problematic for visa applicants who are already in the United States and the U.S. persons in their social networks.[23]

As Justice Sotomayor argued in *Jones*, "[a]wareness that the Government may be watching chills associational and expressive freedoms. And the Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse." *Jones*, 565 U.S. at 416 (Sotomayor, J., concurring).[24] She expressed concern when such data is "the sum of one's public movements" and the government has "recorded and aggregated [it] in a manner that

[23] Compl. [ECF No. 1] ¶¶ 1, 43.

[24] *See also* Compl. [ECF No. 1] ¶ 2.

enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on." *Id. See also NAACP v. Alabama*, 357 U.S. 449, 462 (1958) ("This Court has recognized the vital relationship between freedom to associate and privacy in one's associations."); *Talley v. California*, 362 U.S. 60, 64 (1960) ("Persecuted groups and sects from time to time throughout history have been able to criticize oppressive practices and laws either anonymously or not at all."); *McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334, 357 (1995) ("Anonymity is a shield from the tyranny of the majority."); *Packingham*, 137 S. Ct. at 1735-36 ("[S]ocial media users employ these websites to engage in a wide array of protected First Amendment activity on topics as diverse as human thought.") (internal quotations and citation omitted).

The chilling effects of the Registration Requirement may include visa applicants curtailing or altering their social media habits, or completely disengaging from social media altogether; disassociating from certain individuals if there is a fear that having such connections may be offensive to the U.S. government; or forgoing travel to the United States. Visa applicants who use social media anonymously or pseudonymously may be more inclined to shut down their social media accounts altogether, as they may fear that their social media alter egos will be linked to their real-world identities if they seek to travel to the United States. This risk is particularly acute given that the U.S. government may share social media information with repressive foreign governments.[25] Individuals in visa applicants' social networks, including U.S. persons, may also limit, change, or stop using social media, or sever online connections with

[25] Compl. [ECF No. 1] ¶ 60.

friends, family members, or colleagues who may be applying for a U.S. visa for fear of being under the government's watchful eye.[26]

Studies that have examined the consequences of digital surveillance by the government confirm these chilling effects. Citizen Lab, an interdisciplinary laboratory based at the Munk School of Global Affairs & Public Policy at the University of Toronto, found that 62 percent of study respondents would be less likely to "speak or write about certain topics online" if they knew the government was engaged in online surveillance, with even higher numbers for younger users.[27] A Pew Research Center survey found that 34 percent of those respondents who were aware of the online surveillance programs revealed by Edward Snowden took at least one step to shield their information from the government, such as using social media less often, uninstalling apps, and avoiding use of certain terms in online communications.[28]

When considering the chilling effects of Defendants' social media surveillance program, it makes little difference that the government "acknowledges that some applicants may transition their social media accounts from public-facing to protected, non-public settings."[29] In fact, some visa applicants may hesitate to make their social media profiles wholly private for fear that doing so may negatively impact their visa determination.[30] Visa applicants who use social media

---

[26] Compl. [ECF No. 1] ¶¶ 51, 53-56.

[27] Jonathan W. Penney, *Internet Surveillance, Regulation, and Chilling Effects Online: A Comparative Case Study*, INTERNET POL'Y REV. 6:2 at 8, 18 (2017), https://policyreview.info/articles/analysis/internet-surveillance-regulation-and-chilling-effects-online-comparative-case.

[28] Lee Rainie & Mary Madden, *Americans' Privacy Strategies Post-Snowden*, PEW RES. CTR. (March 16, 2015), https://www.pewresearch.org/internet/2015/03/16/americans-privacy-strategies-post-snowden.

[29] *DS-160 Supporting Statement* at 14 & *DS-260 Supporting Statement* at 13, *supra* note 8.

[30] In an analogous context, travelers carrying devices wiped of any personal information have reported facing heightened scrutiny by border agents who believed such devices indicate that travelers have something to hide. *See, e.g.*, Rob Salerno, *US Customs block Canadian man after*

anonymously or pseudonymously may be loath to maximize privacy settings because the very point is to speak publicly, especially about controversial or sensitive issues.

Finally, it makes little difference that the government promises not to use certain information, including information obtained outside the scope of application forms, in making visa determinations. Defendants attempt to reassure applicants that "visas may not be denied on the basis of race, religion, ethnicity, national origin, political views, gender, or sexual orientation."[31] But the simple fact that the government has *reviewed* personal information is enough to create a chilling effect. Further, it is not unreasonable to fear that information such as political beliefs gleaned from social media profiles may tacitly influence consular officers' visa decisions, even if contrary to policy.[32]

II. Social Media Platforms Can Reveal Vast Amounts of Personal Information About Users

A. Social Networks Are Intricate and Complex

A visa applicant's social media profiles can paint an alarmingly detailed picture of their personal lives, as well as those of their friends, family members, and other connections—many

---

reading his Scruff profile, XTRA (Feb. 20, 2017) ("They said, 'Next time you come through, don't have a cleared phone,' and that was it."), https://www.dailyxtra.com/us-customs-block-canadian-man-after-reading-his-scruff-profile-73048.

[31] *DS-160 Supporting Statement* at 10 & *DS-260 Supporting Statement* at 10, *supra* note 8.

[32] Defendant DHS's component agency CBP has faced numerous allegations of profiling based on social media activity, contrary to the agency's policies. In August 2019, a Palestinian student starting his freshman year at Harvard University was denied entry to the United States allegedly because of the political views *his friends* expressed on social media. Karen Zraick & Mihir Zaveri, *Harvard Student Says He Was Barred From U.S. Over His Friends' Social Media Posts*, N.Y. TIMES (Aug. 27, 2019), https://www.nytimes.com/2019/08/27/us/harvard-student-ismail-ajjawi.html. In January 2020, after the United States' assassination of Iranian General Qasem Soleimani, several Iranians and Iranian Americans alleged that they were questioned about their political views and social media activity at the U.S.-Canada border. *Iranian-Americans 'harassed' by US border officials*, BBC NEWS (Jan. 6, 2020), https://www.bbc.com/news/world-us-canada-51011029.

of whom may be U.S. persons. This is because of the fundamentally interconnected nature of social networks.

Social media can reveal information about a visa applicant in two ways: 1) by the applicant themselves through, for example, biographical information, text-based posts, photos, videos, and group memberships; and 2) by their social media associates via tagging, commenting, and following. Consider the example of how social media may reveal a visa applicant's political beliefs. The visa applicant may share their political beliefs in their biographical information, through membership in a public Facebook group supporting their political party, or by liking a political candidate's Facebook page or following the candidate on Twitter. Their associates may tag the applicant in a political rant or post photos at a political rally that identify the applicant.

Social media can also reveal information about the individuals in a visa applicant's network, including U.S. persons. Information about another user (Friend A) can be revealed by the user themselves or by the visa applicant, as described above, *or* by a third-party associate; for example, the visa applicant posts a photo from a political rally and Friend B tags Friend A in that photo.

There are ways that social media can reveal information about a visa applicant or their associates without *any* party affirmatively sharing that information. Studies have found that even when a user does not explicitly share or indicate the nature of their relationship with their "friends" or "followers" on social media, sexual orientation[33] and romantic relationships[34] can

[33] Carter Jernigan & Behram F.T. Mistree, *Gaydar: Facebook friendships expose sexual orientation*, FIRST MONDAY (Sept. 22, 2009), https://firstmonday.org/article/view/2611/2302.

[34] Brady Robards & Siân Lincoln, *Making It "Facebook Official": Reflecting on Romantic Relationships Through Sustained Facebook Use*, SOC. MEDIA + SOC'Y (Oct. 12, 2016), https://journals.sagepub.com/doi/10.1177/2056305116672890.

reliably be inferred. One study even found that it is possible to predict personal information about *nonusers* of social media based on personal data and contact lists shared by users.[35] As the study put it, "[t]he persistent trace of our online social interaction can slowly accumulate enough data to effectively diminish the decision power of an individual to keep personal information private."[36]

Importantly, while social media users often affirmatively make personal information public, a user may publish personal information unintentionally given the complexities of privacy settings. From organ donation[37] to word processing software,[38] studies show that most people do not change default settings. Even when they do, younger people are more likely to take advantage of available settings than adults over 50.[39] On some social media platforms, it can be difficult to discern exactly what information is public by default.[40] Privacy settings also vary widely across social media platforms, with some offering more granularity than others. *See infra* Part II.B. Additionally, privacy settings can change without warning.[41]

---

[35] Garcia, *supra* note 17.

[36] *Id.*

[37] Shai Davidai, Thomas Gilovich, Lee D. Ross, *The Meaning of Default Options for Potential Organ Donors*, PROCEEDINGS OF THE NAT'L ACAD. SCI. 109:38 (Sept. 18, 2012), https://stanford.app.box.com/s/yohfziywajw3nmwxo7d3ammndihibe7g.

[38] Jared Spool, *Do users change their settings?*, UIE (Sept. 14, 2011), https://archive.uie.com/brainsparks/2011/09/14/do-users-change-their-settings.

[39] Mary Madden & Aaron Smith, *Reputation Management and Social Media*, PEW RES. CTR. (May 26, 2010), https://www.pewresearch.org/internet/2010/05/26/reputation-management-and-social-media.

[40] *See, e.g., Add and Edit Your Profile Info*, FACEBOOK HELP CTR. (explaining how to change various settings without consistently explaining what information is public by default), https://www.facebook.com/help/1017657581651994.

[41] Will Oremus, *Facebook Changed 14 Million People's Privacy Settings to "Public" Without Warning*, SLATE (June 7, 2018), https://slate.com/technology/2018/06/facebook-changed-14-million-peoples-privacy-settings-to-public-without-warning-due-to-a-bug.html.

B. The Fundamentals of Three Popular Social Networks

This section examines three popular social media platforms subject to the Registration Requirement: Facebook, Instagram, and Twitter.

1. Facebook

Facebook is a general-purpose social media platform with 2.6 billion monthly active users[42] who post 350 million photos per day and generate four million "likes" per minute.[43]

Profiles on Facebook always publicly display the user's real or "authentic" name,[44] profile photo, cover photo, references to the user's gender pronouns (he, she, or them), username,[45] and user ID or account number.[46] Users may add biographical information, with occasional nudges from Facebook encouraging them to fill out any fields left blank. These fields include the user's website, gender pronouns, languages they speak, the gender or genders the user is romantically interested in, relationship status, family members, work history, education history, and places they have lived, which are all public by default. Fields for a user's religious views, political views, email address, and address are visible to the user's friends by default. The user's birthday is visible to the user's friends, and friends of friends, by default. The user's gender (male, female, or a custom blank textbox for the user to fill in) is visible only to the user

[42] Dan Noyes, *The Top 20 Valuable Facebook Statistics—Updated May 2020*, ZEPHORIA DIGITAL MARKETING (May 2020), https://zephoria.com/top-15-valuable-facebook-statistics.

[43] Smith, *supra* note 10.

[44] *What names are allowed on Facebook?*, FACEBOOK HELP CTR., https://www.facebook.com/help/112146705538576.

[45] *Your Username*, FACEBOOK HELP CTR., https://www.facebook.com/help/1740158369563165.

[46] *What is public information on Facebook?*, FACEBOOK HELP CTR., https://www.facebook.com/help/203805466323736.

themselves by default. The default settings for profile information are not codified in Facebook's help pages, making it challenging for users to understand what is public by default.[47]

A Facebook profile also includes a reverse-chronological list of posts the user has recently published or interacted with, known as a "timeline." The posts on a user's timeline can contain text, photos, videos, location metadata,[48] a timestamp, and a "tag" or link to other users' profiles. Users can also share albums of photos, which may include location metadata, a timestamp, and tags to other users.[49] In some cases, Facebook will suggest when and where a photo was taken when the user uploads the photo,[50] and even who to tag based on its face recognition algorithm.[51]

The timeline may also include posts made by others directly on the user's timeline,[52] or by people in the user's network who have tagged the user their posts.[53] By default, posts on a user's timeline are visible to the user's friends.[54] Being tagged by others will cause a post to appear on a user's timeline by default. Thus, when User A (or any other user) tags User B in a

---

[47] *Add and Edit Your Profile Info*, FACEBOOK HELP CTR., https://www.facebook.com/help/1017657581651994.

[48] *How do I tag my friends at a location on Facebook?*, FACEBOOK HELP CTR., https://www.facebook.com/help/201009576609790.

[49] *How do I create an album on Facebook?*, FACEBOOK HELP CTR., https://www.facebook.com/help/1898942430347350.

[50] *How is Facebook able to suggest when and where my photo was taken?*, FACEBOOK HELP CTR., https://www.facebook.com/help/387124901306972.

[51] *What is the face recognition setting on Facebook and how does it work?*, FACEBOOK HELP CTR., https://www.facebook.com/help/122175507864081.

[52] *How do I control who can see posts that friends make on my timeline on Facebook?*, FACEBOOK HELP CTR., https://www.facebook.com/help/246629975377810.

[53] *How do I control who sees posts and photos that I'm tagged in on my Facebook timeline?*, FACEBOOK HELP CTR., https://www.facebook.com/help/267508226592992.

[54] *When I tag someone in a post or photo, who can see it?*, FACEBOOK HELP CTR., https://www.facebook.com/help/240051956039320.

post, User B's friends will automatically be able to view User A's post, unless User A has specifically disabled this feature,[55] or User B removes the post[56] or turns on the "tag review" feature to approve tagged posts before they appear.[57] Even when a user chooses to hide a post from their own timeline, that post may still be found through search or on the timeline of the user who posted it or another user who is tagged.[58]

Other users may interact with posts and photos through "comments," "likes," and other reactions.[59] Comments include a timestamp and the commenting user's profile picture, which links to their own profile and all of their biographical information that may be made public. A user with permission to view a post will be able to see the list of users who have liked the post.[60]

Users make connections on Facebook by "friending" each other. These connections are mutual, meaning that both people have assented to the connection. A user's list of "friends" is public by default.[61]

Facebook users can also connect through "groups," usually formed around a common interest, geographic location, activity, or condition.[62] For example, support groups for illness,

---

[55] *Id.*

[56] *How do I remove a tag from a photo or post I'm tagged in on Facebook?*, FACEBOOK HELP CTR., https://www.facebook.com/help/140906109319589.

[57] *How do I review tags that people add to my Facebook posts before they appear?*, FACEBOOK HELP CTR., https://www.facebook.com/help/247746261926036.

[58] *Something I hid from my Timeline is showing up in search on Facebook*, FACEBOOK HELP CTR., https://www.facebook.com/help/159724647510060.

[59] *Who can like or comment on things that I post on Facebook?*, FACEBOOK HELP CTR., https://www.facebook.com/help/167598583302066.

[60] *What does it mean to "Like" something on Facebook?*, FACEBOOK HELP CTR., https://www.facebook.com/help/110920455663362.

[61] *Who can see the Friends section of my Facebook profile?*, FACEBOOK HELP CTR., https://www.facebook.com/help/115450405225661.

[62] *Groups*, FACEBOOK HELP CTR., https://www.facebook.com/help/1629740080681586.

infertility, and other medical conditions are common and explicitly promoted by Facebook.[63] A user's profile may publicly list the groups they are part of, and groups themselves may publicly list their administrators and full membership. The group's administrators and moderators, which the user may be a part of, are listed publicly by default.[64] Only group administrators can change a group's privacy settings, so rank-and-file group members cannot control these settings.[65]

Additionally, Facebook allows users to create and contribute to fundraisers. Facebook's policies claim that a user's contribution to a fundraiser (though not the amount) will only appear to their friends if the user chooses to share it.[66] However, examination of this feature in April 2020 demonstrated that the contribution appears on the user's timeline publicly by default, unless the user changes its visibility settings.

2. Instagram

Instagram is a platform for sharing photographs and audio and video recordings. It has over one billion monthly active users who generate over 100 million posts per day.[67]

Instagram profiles reveal similar information about users and their contacts as Facebook profiles, with images rather than text as their main form of content. An Instagram profile shows a user's username, name, photo, short biography, posts, captions, ephemeral "stories" (posts that

---

[63] *Introducing Changes to Group Types*, FACEBOOK COMMUNITY (Apr. 23, 2019), https://www.facebook.com/community/whats-new/introducing-changes-to-group-types.

[64] *What are the privacy options for Facebook groups?*, FACEBOOK HELP CTR., https://www.facebook.com/help/220336891328465.

[65] *What's the difference between a public and private Facebook group and how do I change the privacy setting?*, FACEBOOK HELP CTR., https://www.facebook.com/help/286027304749263.

[66] *Will my donation on Facebook be seen by my friends?*, FACEBOOK HELP CTR., https://www.facebook.com/help/176532799208393.

[67] Salman Aslam, *Instagram by the Numbers: Stats, Demographics & Fun Facts*, OMNICORE (Feb. 10, 2020), https://www.omnicoreagency.com/instagram-statistics.

disappear after 24 hours), saved stories, as well as lists of profiles the user is "following" and the user's own "followers."

A user's profile also shows photos and videos that the user has been "tagged" in.[68] When User A is tagged in a post by User B, that post will appear in a section of User A's profile by default.[69] User A can choose to remove themselves from individual posts that they have been tagged in.[70]

Compared to Facebook, Instagram offers less granularity in the control users have over the visibility of their content. An Instagram user's entire account is public by default, but the user can choose to set their account to private, in which case only approved followers will be able to see the content that they have shared, their followers list, and the list of people whom they are following.[71] The user's username, name, profile picture, and biography are always publicly available.

In contrast to Facebook's symmetrical friend relationships, connections on Instagram are asymmetrical: User A can follow User B without User B reciprocating. However, if User A's profile is set to private, User A has to approve User B's request to follow.[72]

Other users may interact with posts through "comments" and "likes." The ability for

---

[68] *Who can see the photos and videos I've been tagged in on my Instagram profile?*, INSTAGRAM HELP CTR., https://help.instagram.com/153434814832627.

[69] *Where can I see photos and videos I've been tagged in on Instagram?*, INSTAGRAM HELP CTR., https://help.instagram.com/167099750119914.

[70] *How do I remove myself from a photo or video someone tagged me in on Instagram?*, INSTAGRAM HELP CTR., https://help.instagram.com/178891742266091.

[71] *How do I set my Instagram account to private so that only approved followers can see what I share?,* INSTAGRAM HELP CTR., https://help.instagram.com/448523408565555.

[72] *Managing Your Followers*, INSTAGRAM HELP CTR., https://help.instagram.com/269765046710559.

others to comment can be turned off by the user for individual posts.[73] A comment includes a general timestamp of how many days or weeks ago it was published, as well as the commenting user's profile picture, which links to their own profile. If a user has permission to view the post, they will be able to see the list of users who have liked or commented on it.

3. Twitter

Twitter is a micro-blogging platform with over 330 million monthly active users who publish 500 million "tweets" per day.[74] Compared to platforms like Facebook and Instagram, Twitter is typically used for public posts and conversations, with notable userbases including journalists, elected officials, and celebrities.

A Twitter profile includes the user's username and name, profile picture, cover photo, short biography, location, and website.[75] A profile also shows posts ("tweets") the user has made, and others' tweets the user has shared ("retweeted") or "liked." Lists of profiles the user is "following," as well as the user's own "followers," are also visible.[76]

Twitter's privacy granularity, like Instagram, is available only at the account level, rather than at the level of individual posts.[77] Only 13 percent of U.S. adult Twitter users keep their

[73] *How do I turn comments on or off for my Instagram posts?*, INSTAGRAM HELP CTR., https://help.instagram.com/1766818986917552.

[74] Kit Smith, *60 Incredible And Interesting Twitter Stats And Statistics*, BRANDWATCH (Jan. 2, 2020), https://www.brandwatch.com/blog/twitter-stats-and-statistics/.

[75] *How to customize your profile*, TWITTER HELP CTR., https://help.twitter.com/en/managing-your-account/how-to-customize-your-profile.

[76] *Following FAQs*, TWITTER HELP CTR., https://help.twitter.com/en/using-twitter/following-faqs.

[77] *About public and protected Tweets*, TWITTER HELP CTR., https://help.twitter.com/en/safety-and-security/public-and-protected-tweets.

accounts private.[78] A Twitter user's username and name, profile picture, cover photo, biography, location, website, and the month and year that they joined Twitter are always publicly available.[79]

As on Instagram, Twitter's following and follower relationships are asymmetrical, and do not require reciprocation.[80] If a user's account is set to private, they have to approve other users' requests to follow.

Twitter's tagging system uses "mentions" and "replies." When User A is mentioned in User B's tweet, this does not show up on User A's profile, but it is possible to search for tweets that mention User A.[81] Twitter's replies function similarly to comments on Facebook and Instagram. When viewing a user's tweet, one can see replies to that original post from other users. All replies that a user makes to others' tweets, regardless of the privacy settings of the person the user is replying to, appear on the "Tweets & replies" tab of the user's profile. But if a user's account is set to private, only approved followers can view the user's replies to others' tweets.[82]

When User A retweets User B's posts, those posts also appear on User A's profile. Retweeting is regularly done for commentary purposes, and often does not imply that the user

---

[78] Emma Remy, *How Public and Private Twitter Users in the U.S. Compare—and Why It Might Matter for Your Research*, PEW RES. CTR. (July 15, 2019), https://medium.com/pew-research-center-decoded/how-public-and-private-twitter-users-in-the-u-s-d536ce2a41b3.

[79] *About profile visibility settings*, TWITTER HELP CTR., https://help.twitter.com/en/safety-and-security/birthday-visibility-settings.

[80] *Following FAQs*, *supra* note 76.

[81] *About replies and mentions*, TWITTER HELP CTR., https://help.twitter.com/en/using-twitter/mentions-and-replies.

[82] *Id.*

agrees with the views, as exemplified by the common phrase "retweets are not endorsements."[83]

CONCLUSION

Visa applicants and those in their social networks have privacy and related free speech interests in shielding their public profiles from Defendants' sweeping social media surveillance program. The intricately networked nature of modern social media platforms virtually guarantees that visa applicants are not the only ones burdened by the Registration Requirement—so, too, are their social media connections, many of whom may be U.S. persons. With knowledge that the U.S. government—and perhaps other governments, if data is shared—can review and collect vast amounts of personal information about them, visa applicants and their friends, followers, and those whom the applicants are following may be chilled from freely engaging in speech and associational activities on these platforms. This is particularly concerning in light of the fact that some publicly available social media content may have been shared by a user unintentionally or shared by the user's connections, given the complexities of how social media platforms function, including their varying and changing privacy settings. Moreover, much of this information is outside the scope of the visa application process or may be an inaccurate reflection of the applicant.

For the foregoing reasons, *amicus curiae* Electronic Frontier Foundation urges this Court to deny Defendants' motion to dismiss.

[83] Charlie Warzel, *Meet the Man Behind Twitter's Most Infamous Phrase*, BUZZFEED NEWS (April 15, 2014), https://www.buzzfeednews.com/article/charliewarzel/meet-the-man-behind-twitters-most-infamous-phrase.

Dated: May 28, 2020

Respectfully submitted,

/s/ *Mitchell L. Stoltz*
Mitchell L. Stoltz
Sophia Cope (*pro hac vice* application pending)
Saira Hussain (*pro hac vice* application pending)
Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94109
sophia@eff.org
saira@eff.org
(415) 436-9333 phone
(415) 436-9993 fax

Counsel for Amicus Curiae Electronic Frontier Foundation