ORAL ARGUMENT NOT YET SCHEDULED

Case No. 23-5232

UNITED STATES COURT OF APPEALS

FOR THE DISTRICT OF COLUMBIA CIRCUIT

Doc Society and International Documentary Association,

Plaintiffs-Appellants,

v.

Antony J. Blinken, in his official capacity as Secretary of State, and Alejandro N. Mayorkas, in his official capacity as Secretary of Homeland Security,

Defendants-Appellees.

Appeal from the United States District Court for the District of Columbia,
No. 1:19-cv-03632-TJK
Hon. Timothy J. Kelly

BRIEF OF AMICUS CURIAE ELECTRONIC FRONTIER FOUNDATION IN SUPPORT OF PLAINTIFFS-APPELLANTS AND REVERSAL

Sophia Cope
Saira Hussain
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109-7701
Tel: (415) 436-9333
sophia@eff.org

Attorneys for Amicus Curiae
Electronic Frontier Foundation

CERTIFICATE AS TO PARTIES, RULINGS, RELATED CASES AND STATUTES

Pursuant to D.C. Circuit Rules 26.1 and 28(a)(1) and Fed. R. App. P. 26.1 the Undersigned counsel certifies as follows:

A. Parties and Amici

All parties and intervenors appearing before the district court and in this Court are listed in the Brief for Plaintiffs-Appellants. All *amici* that appeared before the district court are listed in the Brief for Plaintiffs-Appellants. The Electronic Frontier Foundation filed a notice of intent to participate in this appeal as *amicus curiae* on February 1, 2024.

B. Rulings Under Review

References to the rulings at issue appear in the Brief for Plaintiffs-Appellants.

C. Related Cases

The appealed ruling has not previously been before this Court or any other court. There are no related cases pending before this Court or any other court of which counsel is aware.

February 7, 2024

/s/ Sophia Cope
Sophia Cope

Attorney for Amicus Curiae
Electronic Frontier Foundation

CORPORATE DISCLOSURE STATEMENT

Pursuant to D.C. Circuit Rule 26.1 and Federal Rule of Appellate Procedure 26.1, *amicus* submits the following corporate disclosure statement: *Amicus* Electronic Frontier Foundation ("EFF") is a donor-funded, nonprofit civil liberties organization. EFF has no parent corporation, and does not issue stock.

February 7, 2024

/s/ Sophia Cope
Sophia Cope

GLOSSARY OF ABBREVIATIONS

Pursuant to D.C. Circuit Rule 28(a)(3), the following is a glossary of abbreviations and acronyms used in this brief.

CBP	Customs and Border Protection
DHS	Department of Homeland Security
EFF	Electronic Frontier Foundation
JA	Joint Appendix

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

Cases

Other Authorities

*Authorities upon which we chiefly rely are marked with asterisk

STATEMENT OF IDENTITY AND INTEREST OF AMICUS CURIAE AND SOURCE OF AUTHORITY TO FILE

The Electronic Frontier Foundation ("EFF") is a non-profit civil liberties organization with more than 31,000 dues-paying members that has worked for 30 years to ensure that technology supports freedom, justice, and innovation for all people of the world. EFF is particularly concerned with technological advances resulting in new government power to pry into the private lives and expressive activities of people within and outside of the United States.

Pursuant to D.C. Circuit Rule 29(b), EFF certifies that all parties have consented to the filing of this *amicus* brief.

Pursuant to D.C. Circuit Rule 29(b), EFF certifies that this separate *amicus* brief is necessary because *amicus* offers the Court additional perspectives on the privacy interests that individuals have in publicly-facing social media profiles.

STATEMENT OF AUTHORSHIP AND FINANCIAL CONTRIBUTIONS

Pursuant to Federal Rule of Appellate Procedure 29(a)(4)(E), EFF states that no party or party's counsel authored this brief in whole or in part, or contributed money that was intended to fund preparing or submitting this brief. No person other than *amicus*, its members, or its counsel contributed money that was intended to fund preparing or submitting 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). Over 75 percent of the world's population age 13 and older uses social media—4.74 billion people.[1] Seventy-two percent of Americans do, too.[2] "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).

Defendants' social media surveillance program, enabled by the Disclosure Requirement,[3] targets the publicly available information on social media profiles of visa applicants, many of whom are already in the United States. When viewed comprehensively, such content reveals vast amounts of users' personal details. To prying eyes, including those of the government, social media can be a gold mine for surveillance. Indeed, as Justice Sotomayor recognized, "the

---

[1] Claire Beveridge & Sam Lauron, *160+ Social Media Statistics Marketers Need for 2023*, Hootsuite (Jan. 26, 2023), https://blog.hootsuite.com/social-media-statistics-for-social-media-managers/.

[2] *Social Media Fact Sheet*, Pew Research Center (Apr. 7, 2021), https://www.pewresearch.org/internet/2021/04/07/social-media-use-in-2021/.

[3] The "Disclosure Requirement" compels visa applicants to "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." JA010–11 (Compl. ¶ 1). Social media identifiers are synonymous with usernames.

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).

User privacy is further frustrated when personal information is publicly revealed without users voluntarily sharing it. Due to the networked nature of social media, users' personal information may not be published by users themselves, but by their social media connections. Even when users publicly post personal information on social media, they may do so inadvertently due to the complexities of privacy settings.

Defendants' social media surveillance program does not solely affect visa applicants; it also implicates those in their social networks, many of whom may be U.S. persons. This amounts to millions, if not billions, of people, given that the Disclosure Requirement applies to an estimated 14.7 million visa applicants annually.[4]

---

[4] JA010–11 (Compl. ¶ 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-

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, they will less freely engage in speech and association on social media platforms like Facebook, Instagram, and X (formerly Twitter).

Visa applicants may be chilled out of fear that they could be denied a visa—or a visa renewal, as the district court at least partially recognized. *See* JA362. Visa applicants *and* those in their social networks may be chilled by the simple fact that the U.S. government is reviewing vast amounts of their personal information—including political beliefs, sexual orientation, or the identity of their friends and family. "The characteristics of modern communications technology that enhance association … also enhance the potential that association will be chilled by relational surveillance."[5] These chilling effects are heightened because Defendants are not just collecting publicly available social media information, but may also be storing it for decades, using it for other

---

06490/60-day-notice-of-proposed-information-collection-application-for-immigrant-visa-and-alien.

[5] Katherine J. Strandburg, *Freedom of Association in a Networked World: First Amendment Regulation of Relational Surveillance*, 49 B.C. L. Rev. 741, 751 (2008).

purposes, and sharing it with other governmental entities.[6]

For these reasons, *amicus* urges this Court to reverse the district court's order and remand the case for further proceedings.

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, despite the Disclosure Requirement only targeting "public-facing" social media.[7] Defendants can view 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. Courts must reject a "cramped notion of personal privacy" as it relates to First Amendment rights because modern digital technology makes surveillance and data compilation easier and cheaper, threatening "the individual's control of information concerning his or her person." *See U.S. Dept. of Justice v. Reporters Committee for Freedom of Press ("RCFP")*, 489 U.S.

---

[6] JA023–24 (Compl. ¶¶ 35-37).

[7] 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*, at 21 (April 10, 2019), https://www.reginfo.gov/public/do/PRAViewDocument?ref_nbr=201808-1405-009.

749, 763 (1989).

A. Defendants' Broad Social Media Surveillance Program Gives the Government an "Easy and Cheap" Way to Compile Users' Personal Information

Modern digital technologies are unprecedented: they chronicle in persistent, exhaustive, and minute detail all aspects of individuals' lives. Social media platforms can publicly reveal—and thus the government can easily gather—vast amounts of personal information, implicating users' privacy interests.

Notably, Defendants have only limited their social media surveillance program to review of publicly available content. While visa applicants must report the social media platforms they have *used* in the past five years, Defendants are not limited to only looking at social media content *date stamped* during that period.[8]

Internet platforms host massive amounts of data. Even more than a 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.[9]

---

[8] JA020 (Compl. ¶ 28); *DS-160 Supporting Statement* at 22 & *DS-260 Supporting Statement* at 20, *supra* n.7.

[9] For instance, Meta, Facebook's parent corporation, has 21 data centers worldwide, spanning 40 million square feet. Meta, Data Centers,

This is far *more* than what *Riley* contemplated for cell phones: "Sixteen gigabytes translates to millions of pages of text, thousands of pictures, or hundreds of videos." *Id.* at 394. *Riley* noted, for example, that "[t]he sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions." *Id.* This and more are often publicly available on social media platforms. *See infra* Part II.B.

Social media profiles also contain personal information that can reveal, directly and inferentially, "a wealth of detail about [individuals'] familial, political, professional, religious, and sexual associations." *See Jones*, 565 U.S. at 415 (Sotomayor, J., concurring). Social media's "time-stamped data provides an intimate window into a person's life," *see Carpenter v. United States*, 138 S.Ct.

---

https://datacenters.atmeta.com/; Rich Miller, *Facebook Showcases its 40 Million Square Feet of Global Data Centers*, Data Center Frontier (Sept. 15, 2021), https://www.datacenterfrontier.com/hyperscale/article/11427952/facebook-showcases-its-40-million-square-feet-of-global-data-centers. One such facility in Utah reportedly can hold between 3 and 12 exabytes of data. Art Raymond, *Facebook data farm in Eagle Mountain is expanding, as are its tax breaks*, Deseret News (Feb. 11, 2021), https://www.deseret.com/utah/2021/2/11/22277090/facebook-server-farm-social-media-tax-breaks-public-subsidy-big-tech-eagle-mountain. Each exabyte is one billion gigabytes. By comparison, smartphones hold some 100 gigabytes. Andy Walker, *The average Android phone offered nearly 100GB storage in 2020*, Android Authority (Mar. 30, 2021), https://www.androidauthority.com/average-smartphone-storage-1213428.

2206, 2217 (2018), and even their personality.[10] This allows the government to derive personal information that it may not otherwise have access to via the visa application alone. For example, Form DS-260 rightfully does not ask visa applicants for political beliefs.[11] Yet political beliefs may be easily ascertainable from public social media content. *See infra* Part II.A. Thus, "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.

Digital technologies also enable the compilation of previously uncompiled information.[12] Social media platforms "collect[] in one place many distinct types of information … that reveal much more in combination than any isolated record." *See Riley*, 573 U.S. at 394. Hundreds or thousands of social media posts may also include photos and videos, group memberships, and other unique

---

[10] Gwendolyn Seidman, *What Can We Learn About People From Their Social Media?,* Psychology Today (Sept. 21, 2020), https://www.psychologytoday.com/us/blog/close-encounters/202009/what-can-we-learn-about-people-their-social-media.

[11] *DS-160 Supporting Statement* at 10 & *DS-260 Supporting Statement* at 10, *supra* n.7. *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] For example, Customs and Border Protection ("CBP"), a component of the Department of Homeland Security ("DHS"), uses a digital tool to "link a person's Social Security number to their social media posts and location data." Joseph Cox, *Homeland Security Uses AI Tool to Analyze Social Media of U.S. Citizens and Refugees*, Vice (May 17, 2023), https://www.vice.com/en/article/m7bge3/dhs-uses-ai-tool-babel-x-babel-street-social-media-citizens-refugees.

data—which collectively reveal much more than a few discrete pieces of content.[13] Moreover, the government here is collecting data *across* different social media platforms. It is "the power of compilations to affect personal privacy that outstrips the combined power of the bits of information…." *See RCFP*, 489 U.S. at 765.

The breadth of Defendants' social media surveillance program is also measured by the sheer number of people affected. This includes visa applicants *and* those in their social networks, including U.S. persons.[14] Defendants admit that the Disclosure Requirement affects 14.7 million visa applicants annually.[15] Their social media connections are many millions more. Facebook's Cambridge Analytica scandal[16] revealed how surveillance of a small set of users can invade

---

[13] The government can also obtain personal information from data brokers, which themselves aggregate data from social media posts, as well as public records and other sources. *See* Justin Sherman, *How Shady Companies Guess Your Religion, Sexual Orientation, and Mental Health*, Slate (April 26, 2023), https://slate.com/technology/2023/04/data-broker-inference-privacy-legislation.html. CBP is "among a wide range of federal agencies known to purchase Americans' private data" from data brokers. Dell Cameron, *How the US Can Stop Data Brokers' Worst Practices—Right Now*, Wired (Feb. 8, 2023), https://www.wired.com/story/fcra-letter-data-brokers-privacy-regulation/.

[14] Many visa applicants are already in the country and therefore are themselves U.S. persons. JA010–11, JA027 (Compl. ¶¶ 1, 43).

[15] *See supra* n.4.

[16] Cambridge Analytica developed a personality quiz 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*

the privacy of the tens of millions of people in their networks: "Only 270,000 people ever used the This Is Your Digital Life (TIYDL) app, but Facebook estimates that data from 87 million people ended up in the hands of Cambridge Analytica."[17] Importantly, Defendants have not excluded the possibility of collecting information about visa applicants' social media connections, including U.S. persons.[18]

Moreover, digital technologies "make long-term monitoring relatively easy and cheap." *See Jones*, 565 U.S. at 429 (Alito, J., concurring in the judgment). Thus, surveillance of social media—"by making available at a relatively low cost such a substantial quantum of intimate information about any

---

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.

[17] 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 estimates 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.

[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* n.7.

person whom the government, in its unfettered discretion, chooses to track—may alter the relationship between citizen and government in a way that is inimical to a democratic society." *See id.* at 416 (Sotomayor, J., concurring) (citation omitted).

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

Given the broad scope of Defendants' social media surveillance program, visa applicants and their social media connections have significant privacy interests in protecting their digital lives from government scrutiny, even when those lives play out in public posts. The Supreme Court repeatedly has held that the government's collection and compilation of publicly available personal information—especially when enhanced by technology—can burden privacy.

In *RCFP*, the Court held that individuals have "significant" privacy interests in their criminal history summaries, i.e., "rap sheets," compiled by the FBI. *RCFP*, 489 U.S. at 767, 780 (holding that "rap sheets" fall within the privacy exemption of the Freedom of Information Act). The Court emphasized the "practical obscurity" of criminal history data—although public, it is hard to find across various sources. *Id.* at 762, 780. The Court recognized that there are special privacy interests associated with the government's digitized compilations of disparate public data: "Plainly there is a vast difference between the public records that might be found after a diligent search of courthouse files, county

archives, and local police stations throughout the country and a computerized summary located in a single clearinghouse of information." *Id.* at 764.

The Court has extended this reasoning to other types of compilations of publicly available information. In *Jones*, the Court "recognized that individuals have a reasonable expectation of privacy in the whole of their physical movements," including in public. *Carpenter*, 138 S.Ct. at 2217 (citing *Jones*, 566 U.S. at 430 (Alito, J. concurring in the judgment), *id.* at 415 (Sotomayor, J., concurring)). 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 ..." *Id.* As the Court recognized, "a person does not surrender all [constitutional] protection by venturing into the public sphere." *Id*.

Here, the government leverages the technology of social media platforms to surveil visa applicants and potentially their associates. Social media profiles reveal not just users' physical locations over time (whether through location stamps, textual declarations, or implication via photos), as in *Jones* and *Carpenter*, but also myriad other aspects of users' personal lives. Moreover, while consular officers will surely manually scroll through visa applicants' public social media content, they also may use automated tools to increase the

efficiency and comprehensiveness of their review. The State Department has not stated whether it uses such tools, but DHS's component CBP does for its own social media surveillance program.[19]

If individuals have significant privacy interests in their comprehensive "rap sheets," despite the individual data points being publicly available as in *RCFP*, then surely visa applicants and their social media connections have significant privacy interests in their *non-criminal* personal information in publicly available online sources. Indeed, these often expose First Amendment-protected activity. Moreover, Defendants' social media surveillance program is enforced not only during the visa vetting process, but also after visa holders arrive in the United States.[20] 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

[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." CBP, *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* JA032–33 (Compl. ¶ 57) (discussing the risks of "automated review tools").

[20] Visa holders are subject to ongoing social media monitoring by DHS's component agencies. JA025, JA036 (Compl. ¶¶ 38, 63). Additionally, visa holders in the U.S. who seek to renew their visas will again be subject to the Disclosure Requirement. JA018 (Compl. ¶ 23).

entities.[21] Justice Sotomayor identified the constitutional problem when the government acquires data that reflects "the sum of one's public movements," and has "recorded and *aggregated* [it] in a manner that enables the Government to ascertain, more or less at will, [a person's] political and religious beliefs, sexual habits, and so on." *Jones*, 565 U.S. at 416 (Sotomayor, J., concurring) (emphasis added).

Further, much publicly available personal information about a person may not be made public *voluntarily*, due to difficulties in navigating default privacy settings within and across platforms or because a user's social media contacts may publicly reveal their information without their consent.[22] *See infra* Part II.A.

The government's compilation of visa applicants and their associates' personal data as gleaned from social media platforms can amount to an "all-encompassing record," *see Carpenter*, 138 S.Ct. at 2217, and is yet 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).

---

[21] JA023–24 (Compl. ¶¶ 35–37).

[22] *See, e.g.*, *Who can tag me and how do I know if someone tags me on Facebook?*, Facebook Help Ctr. ("You can be tagged in posts and photos by Friends and friends of friends … Remember, posts you choose not to allow on your timeline may appear in Feed and elsewhere on Facebook."), https://www.facebook.com/help/226296694047060/.

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

If social media users know that the government can extrapolate massive amounts of personal information from a comprehensive review of their profiles, and even link their pseudonymous accounts to their real-world identities, those users will likely engage in self-censorship and curtail their online speech and association. This is particularly problematic for visa applicants who are already in the United States and the U.S. persons in their networks.[23]

As Justice Sotomayor argued in *Jones*, "[a]wareness that the government may be watching chills associational and expressive freedoms." 565 U.S. at 416 (Sotomayor, J., concurring).[24] *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.").

The chilling effects of the Disclosure Requirement may include visa

[23] JA010–11, JA027 (Compl. ¶¶ 1, 43).
[24] *See also* JA011 (Compl. ¶ 2).

applicants curtailing or altering their social media habits; completely disengaging from social media; disassociating from individuals for 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 pseudonymously may shut down their social media accounts, for fear they will be linked to their real-world identities. This risk is particularly acute given that the U.S. government may share social media information with repressive foreign governments.[25] Visa applicants' social media connections, including U.S. persons, may also fear the government's watchful eye, leading them to limit or stop using social media, or sever online connections with friends, family, or colleagues who may be applying for a U.S. visa.[26]

Studies examining the consequences of government digital surveillance confirm these chilling effects. Citizen Lab, an interdisciplinary laboratory 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

[25] JA035 (Compl. ¶ 60).

[26] JA029–32 (Compl. ¶¶ 51, 53–56).

younger users.[27] A Pew Research Center survey found that 34 percent of respondents who were aware of the government's digital surveillance programs revealed by Edward Snowden in 2013 took at least one step to shield their information from the government, such as using social media less often, uninstalling apps, or avoiding use of certain terms.[28]

When considering chilling effects, 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 fear that doing so will have a negative impact on their visa determination.[30] Visa applicants who use social media pseudonymously

---

[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* n.7.

[30] Analogously, travelers carrying devices wiped of any personal information have reported heightened scrutiny by CBP agents who believed they must have something to hide. *See, e.g.*, Rob Salerno, *US Customs block Canadian man after reading his Scruff profile*, Xtra (Feb. 20, 2017) ("They said, 'Next time you come through, don't have a cleared phone'"), https://www.dailyxtra.com/us-customs-block-canadian-man-after-reading-his-scruff-profile-73048.

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

Finally, it makes little difference that the government promises not to use 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 government's *review* of personal information is enough to create a chilling effect. Further, it is reasonable to fear that information such as political beliefs gleaned from social media profiles may influence consular officers' visa decisions, even if contrary to policy.[32]

---

[31] *DS-160 Supporting Statement* at 10 & *DS-260 Supporting Statement* at 10, *supra* n.7.

[32] CBP has faced numerous allegations of profiling based on social media activity, contrary to its policies. In August 2019, a Palestinian student at Harvard University was denied entry 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, 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.

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

A. Social Networks Are Intricate and Complex

Because of the fundamentally interconnected nature of social media networks, a visa applicant's public-facing profiles can paint an alarmingly detailed picture of their personal lives, as well as those of their connections. 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 political beliefs. The visa applicant may share their political beliefs in their biographical information or through membership in a public Facebook group supporting a political candidate, or an associate could tag the applicant in a political screed or in photos at a political rally.

Furthermore, social media can also reveal information about other individuals in a visa applicant's network, including U.S. persons. For example, a visa applicant (or a third-party) could tag another user in a post or photo that appears on the visa applicant's profile. Even simply being connected with a visa applicant via social media may draw the government's attention to that connection's profile.

Visa applicants and their associates' personal information can be revealed

through social media without *any* party affirmatively sharing it. Studies have found, for example, that even when a user does not explicitly indicate the nature of their relationships on social media, their romantic relationships[33] and sexual orientation[34] can often 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's author 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]

Additionally, a person may publicly share their personal information inadvertently, due to the complexities and difficulties in navigating privacy settings, which vary widely across social media platforms and differ in granularity. *See infra* Part II.B. Although younger people are more likely to take

---

[33] 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.

[34] Carter Jernigan & Behram F.T. Mistree, *Gaydar: Facebook friendships expose sexual orientation*, First Monday (Sept. 22, 2009), https://firstmonday.org/ojs/index.php/fm/article/view/2611.

[35] David Garcia, *Leaking Privacy and Shadow Profiles in Online Social Networks*, Science Advances (Aug. 4, 2017), https://advances.sciencemag.org/content/3/8/e1701172.

[36] *Id.*

advantage of available settings than adults over 50,[37] studies show that many people do not change default settings.[38] On some social media platforms, it can be difficult to discern exactly what information is public by default.[39] Particularly worrisome, some platforms change privacy settings without warning.[40]

B. The Fundamentals of Three Popular Social Networks

1. Facebook

Facebook is a general-purpose social media platform with 3.05 billion monthly active users[41] who post 350 million photos per day and generate four

---

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

[38] *See* Jon M. Jacchimowicz et al., *When and why defaults influence decisions: a meta-analysis of default effects*, Behavioral Pub. Pol'y 3:2 (Nov. 2019), https://doi.org/10.1017/bpp.2018.43.

[39] *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.

[40] 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.

[41] Brian Dean, *Facebook User and Growth Statistics to Know in 2024*, Backlinko (Dec. 12, 2023), https://backlinko.com/facebook-users#facebook-key-stats.

million "likes" per minute.[42]

Facebook requires users to publicly display the user's real or "authentic" name,[43] profile picture, cover photo, system pronouns (i.e. the pronoun Facebook uses when referring to the user), username, and user ID or account number.[44] Users may add biographical information, including the user's gender pronouns, work history, education history, current city, hometown, relationship status, name pronunciation, website, and social links, which are all public by default. Users can select with whom to share their gender identity (female, male, nonbinary, or more options, which yields a custom blank textbox for the user to fill in).[45] Users can add far more information to a Facebook profile; however, the default settings for most profile information is not explained in Facebook's help pages, making it challenging to understand what is public by default.[46]

---

[42] Kit Smith, *53 Incredible Facebook Statistics and Facts*, Brandwatch (June 1, 2019),https://www.brandwatch.com/blog/facebook-statistics/

[43] *What names are allowed on Facebook?*, Facebook Help Ctr., https://www.facebook.com/help/112146705538576.

[44] *What is public information on Facebook?*, Facebook Help Ctr., https://www.facebook.com/help/203805466323736.

[45] *See Being Your Authentic Self on Facebook*, Facebook Help Ctr., https://www.facebook.com/help/186614050293763. *See also Edit information on your Facebook profile and choose who can see it*, Facebook Help Ctr., https://www.facebook.com/help/276177272409629.

[46] *Add and Edit Your Profile Info*, Facebook Help Ctr., https://www.facebook.com/help/1017657581651994.

A Facebook profile also includes a reverse-chronological list of posts a 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,[47] 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.[48] In some cases, Facebook will suggest when and where a photo was taken when the user uploads the photo.[49]

The timeline may also include posts made by others directly on the user's timeline,[50] or by people in the user's network who have tagged the user in their posts.[51] Being tagged by others will cause a post to appear on a user's timeline by default.[52] Thus, when User A tags User B in a post, User B's friends will automatically be able to view User A's post, unless User A has specifically

---

[47] *How do I tag my friends at a location on Facebook?*, Facebook Help Ctr., https://www.facebook.com/help/201009576609790.

[48] *Create an album on Facebook*, Facebook Help Ctr., https://www.facebook.com/help/1898942430347350.

[49] *How is Facebook able to suggest when and where my photo was taken?*, Facebook Help Ctr., https://www.facebook.com/help/387124901306972.

[50] *Control who can see posts on your Facebook timeline*, Facebook Help Ctr., https://www.facebook.com/help/246629975377810.

[51] *Control who sees posts and photos you're tagged in on Facebook*, Facebook Help Ctr., https://www.facebook.com/help/267508226592992.

[52] *When I tag someone in a post or photo, who can see it?*, Facebook Help Ctr., https://www.facebook.com/help/240051956039320.

disabled this feature,[53] or User B removes the post[54] or turns on the "tag review" feature to approve tagged posts before they appear.[55] Even when a user chooses to hide a post from their own timeline, that post may still be found through the search function or on the timeline of the user who posted it or another user who is tagged.[56]

Other users may interact with posts and photos through "comments," "likes," and other reactions.[57] Comments include a timestamp and the commenting user's profile picture, which links to their own profile and all of their biographical information that has been made public. A user with permission to view a post will be able to see the list of users who have liked the post.[58]

Users make connections on Facebook by "friending" each other, which

---

[53] *Id.*

[54] *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.

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

[56] *Something I hid from my profile is showing up in search on Facebook*, Facebook Help Ctr., https://www.facebook.com/help/159724647510060.

[57] *Who can like or comment on things that I post on Facebook?*, Facebook Help Ctr., https://www.facebook.com/help/167598583302066.

[58] *What does it mean to "Like" something on Facebook?*, Facebook Help Ctr., https://www.facebook.com/help/110920455663362.

requires both people to assent to the connection. A user's list of "friends" is public by default.[59]

Facebook users can also connect through "groups," usually formed around a common interest, geographic location, activity, or condition.[60] 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.[61] Only group administrators can change a group's privacy settings, so rank-and-file group members cannot control these settings.[62]

2. Instagram

Instagram is a platform popular for sharing photographs and video recordings publicly. It has over two billion monthly active users who upload over 1,000 photos per *second*.[63]

---

[59] *Adjust who can see your Friends section on Facebook*, Facebook Help Ctr., https://www.facebook.com/help/115450405225661.

[60] *Groups*, Facebook Help Ctr., https://www.facebook.com/help/1629740080681586.

[61] *Difference between public and private Facebook groups*, Facebook Help Ctr., https://www.facebook.com/help/220336891328465.

[62] *Change a Facebook group from public to private*, Facebook Help Ctr., https://www.facebook.com/help/286027304749263.

[63] Muninder Adavelli, *Instagram Daily Active Users: How Many Use It Daily*, TechJury (July 27, 2023), https://techjury.net/blog/how-many-daily-active-users-on-instagram/.

Instagram profiles reveal similar information about users and their contacts as Facebook profiles, with images rather than text as the main form of content. An Instagram profile shows a user's username, name, profile photo, short biography, website, posts, ephemeral "stories" (posts that 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.[64] When User A is tagged in a post by User B, that post will appear automatically in a section of User A's profile by default.[65] User A can choose to remove themselves from individual posts that they have been tagged in,[66] or change their settings to manually approve all tagged content.[67]

Compared to Facebook, Instagram offers less granularity in the control users have over the visibility of their content. Instagram accounts for users over

---

[64] *Who can see the posts you're tagged in on your Instagram profile*, Instagram Help Ctr., https://help.instagram.com/153434814832627.

[65] *Where to see Instagram posts you're tagged in*, Instagram Help Ctr., https://help.instagram.com/167099750119914; *Choose to manually approve Instagram posts you're tagged in*, Instagram Help Ctr., https://help.instagram.com/496738090375985.

[66] *Remove yourself from a post someone tagged you in on Instagram*, Instagram Help Ctr., https://help.instagram.com/178891742266091.

[67] *Choose to manually approve Instagram posts you're tagged in*, Instagram Help Ctr., https://help.instagram.com/496738090375985.

the age of 16 are public by default, but users can choose to set their account to private, [68] in which case only approved followers can see their content, their full followers list, and the list of people whom they are following.[69] However, even with a private account, the user's username, name, profile photo, and biography are always publicly available.[70]

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.[71]

Other users may interact with posts through "comments" and "likes." The ability for others to comment can be turned off by a user for individual posts.[72] A comment includes a general timestamp of how many days or weeks ago it was published, as well as the commenting user's profile photo, which links to their own profile. If a user has permission to view the post, they will be able to see

---

[68] *Make your Instagram account private*, Instagram Help Ctr., https://help.instagram.com/448523408565555.

[69] *Differences between public and private accounts on Instagram*, Instagram Help Ctr., https://help.instagram.com/517073653436611?helpref=faq_content

[70] *Id*.

[71] *Managing Your Followers*, Instagram Help Ctr., https://help.instagram.com/269765046710559.

[72] *Turn comments on or off for Instagram posts*, Instagram Help Ctr., https://help.instagram.com/1766818986917552.

the list of users who have liked or commented on it.

3. X (Formerly Twitter)

X is a micro-blogging platform with over 436 million monthly active users who publish 500 million "posts" per day.[73] Compared to platforms like Facebook and Instagram, X is typically used for public posts and conversations, with notable userbases including journalists, elected officials, and celebrities.

An X profile includes the user's username and name, profile photo, header image, short biography, location, and website.[74] A profile also shows posts the user has made, and others' posts the user has shared ("reposted") or "liked."[75] Lists of profiles the user is "following," as well as the user's own "followers," are also visible.[76]

X's privacy granularity, like Instagram, is available only at the account level, rather than at the level of individual posts.[77] Accounts are public by

---

[73] Susan Laborde, *55+ Stunning Twitter Statistics You Need to Know in 2023*, Tech Report (July 6, 2023), https://techreport.com/statistics/twitter-statistics/.

[74] *How to customize your profile*, X Help Ctr., https://help.twitter.com/en/managing-your-account/how-to-customize-your-profile.

[75] *See Repost FAQs*, X Help Ctr., https://help.twitter.com/en/using-x/repost-faqs.

[76] *Following FAQs*, X Help Ctr., https://help.twitter.com/en/using-twitter/following-faqs.

[77] *About public and protected Posts*, X Help Ctr., https://help.twitter.com/en/safety-and-security/public-and-protected-posts.

default,[78] and, as of 2019, only 13 percent of U.S. adult Twitter users kept their accounts private.[79] An X user's username and name, profile photo, header image, biography, location, website, and the month and year that they joined X are always publicly available.[80]

As on Instagram, X's following and follower relationships are asymmetrical, and do not require reciprocation.[81] If a user's account is set to private, they must approve other users' requests to follow.

X's tagging system uses "mentions" and "replies." When User A is mentioned in User B's post, this does not show up on User A's profile, but it is possible to search for posts that mention User A.[82] Users' replies on X function similarly to comments on Facebook and Instagram. When viewing a user's post, one can see replies to that original post from other users. All replies that a user makes to others' posts, regardless of the privacy settings of the person the user is

---

[78] *Id.*

[79] 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.

[80] *About profile visibility settings*, X Help Ctr., https://help.twitter.com/en/safety-and-security/birthday-visibility-settings.

[81] *Following FAQs*, *supra* n.76.

[82] *About replies and mentions*, X Help Ctr., https://help.twitter.com/en/using-twitter/mentions-and-replies.

replying to, appear on the "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' posts.[83]

When User A reposts User B's posts, those posts also appear on User A's profile. Reposting is regularly done for commentary purposes, and often does not imply that the user agrees with the views, as exemplified by the common phrase "retweets are not endorsements."[84]

CONCLUSION

For the foregoing reasons, *amicus* urges this Court to reverse the district court's order and remand the case for further proceedings.

February 7, 2024

Respectfully submitted,

By: */s/ Sophia Cope*

Sophia Cope
Saira Hussain
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109-7701
Tel: (415) 436-9333
sophia@eff.org

Attorneys for Amicus Curiae
Electronic Frontier Foundation

[83] *Id.*

[84] 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.

CERTIFICATE OF SERVICE

I hereby certify that on February 7, 2024 I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the District of Columbia Circuit by using the appellate CM/ECF system.

I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the appellate CM/ECF system.

February 7, 2024 *<u>/s/ Sophia Cope</u>*
Sophia Cope

CERTIFICATE OF COMPLIANCE WITH TYPE-VOLUME LIMITATION, TYPEFACE REQUIREMENTS, AND TYPE STYLE REQUIREMENTS PURSUANT TO FED. R. APP. P. 32(G)(1)

I hereby certify as follows:

1. The undersign certifies under Rule 32(g)(1) that this brief complies with the type-volume limitation of Fed. R. App. P. 29(a)(5) and 32(a)(7)(b). The brief is printed in proportionally spaced 14-point type, and the brief has 6,288 words according to the word count of the word-processing system used to prepare the brief (excluding the parts of the brief exempted by Fed. R. App. P. 32(f).

2. The brief complies with the typeface requirements of Federal Rule of Appellate Procedure 32(a)(5), and with the type style requirements of Federal Rule of Appellate Procedure 32(a)(6). The brief has been prepared in a proportionally spaced typeface using Microsoft® Word for Mac 365 in 14-point Times New Roman font.

February 7, 2024

/s/ Sophia Cope
Sophia Cope