No. 19-1116

IN THE
Supreme Court of the United States

LINKEDIN CORP.;

Petitioner,

v.

HIQ LABS, INC.,

Respondent.

On Petition for a Writ of Certiorari to the
U.S. Court of Appeals
for the Ninth Circuit

MOTION FOR LEAVE TO FILE BRIEF AS *AMICUS CURIAE* AND BRIEF OF ELECTRONIC PRIVACY INFORMATION CENTER (EPIC) AS *AMICUS CURIAE* IN SUPPORT OF PETITIONER

MARC ROTENBERG
Counsel of Record
ALAN BUTLER
MEGAN IORIO
ELECTRONIC PRIVACY
INFORMATION CENTER (EPIC)
1519 New Hampshire
Avenue NW
Washington, DC 20036
(202) 483-1140
rotenberg@epic.org

April 13, 2020

MOTION FOR LEAVE TO FILE BRIEF AS *AMICUS CURIAE*

Under Rule 37.2(b), the Electronic Privacy Information Center (EPIC) respectfully moves for leave to file the accompanying brief as *amicus curiae* in support of the petition for a writ of certiorari. In accordance with Rule 37.2(a), both parties were notified of the intent to file this brief ten days prior to the filing date. Petitioner has consented to the filing of this brief, but respondent has not responded to EPIC's request for consent to file.

EPIC is a public interest research center in Washington, D.C. EPIC was established in 1994 to focus public attention on emerging civil liberties issues, to promote government transparency, and to protect privacy, the First Amendment, and other constitutional values.

EPIC has filed several *amicus* briefs in this Court concerning consumer privacy. *See, e.g.*, Brief for EPIC et al. as *Amici Curiae* Supporting Petitioners, *Barr v. Am. Ass. of Political Consultants*, No. 19-631 (U.S. filed Nov. 14, 2019) (arguing that the Telephone Consumer Protection Act is constitutional); Brief for EPIC as *Amicus Curiae* Supporting Respondents, *PDR Network v. Carlton & Harris Chiropractic*, 139 S. Ct. 2051 (2019) (No. 17-1705) (arguing that TCPA defendants should not be able to challenge FCC interpretations of the TCPA outside the review process Congress established); Brief for EPIC et al. as *Amici Curiae* Supporting Respondent, *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540 (2016) (No. 13-1339) (arguing that violation of statutory privacy rights confers Article III standing); Brief of EPIC et al. as *Amici Curiae* Supporting Petitioner, *Maracich v. Spears,* 570 U.S. 48 (2013) (No. 12-25) (arguing that the scope of the litigation exception

to the Driver's Privacy Protection Act should be narrow); Brief for EPIC et al. as *Amici Curiae* Supporting Petitioners, *Sorrell v. IMS Health*, 564 U.S. 552 (2011) (No. 10-779) (arguing that a Vermont law restricting use of prescriber-identifying data protected patient privacy); Brief for EPIC as *Amicus Curiae* Supporting Petitioners, *Reno v. Condon*, 528 U.S. 141 (2000) (No. 98-1464) (arguing that the Driver Privacy Protection Act was consistent with constitutional principles of federalism).

EPIC has a unique interest in this case because the lower court's decision threatens the privacy interests of internet users, who are not represented by either of the parties in this case. EPIC participated as *amicus curiae* in the Ninth Circuit case below. Brief for EPIC as *Amicus Curiae* in Support of Appellant, *hiQ Labs, Inc. v. LinkedIn Corp.*, 938 F.3d 985 (9th Cir. 2019) (No. 17-16783).

EPIC has led the effort to establish consumer privacy safeguards in the United States. For example, EPIC's 2009 Federal Trade Commission complaint concerning Facebook's privacy practices helped establish the agency's historic consent order. Fed. Trade. Comm'n, *Facebook Settles FTC Charges That It Deceived Consumers by Failing to Keep Privacy Promises* (Nov. 29, 2011)[1] ("Facebook's privacy practices were the subject of complaints filed with the FTC by the Electronic Privacy Information Center and a coalition of consumer groups.") EPIC has filed numerous other complaints at the FTC against companies that do not adequately protect user data. *See, e.g., In the Matter of Airbnb, Inc.,* Complaint and Request for Investigation,

---

[1] https://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep.

Injunction, and Other Relief (Feb. 26, 2020) (challenging Airbnb's deployment of a "risk assessment" technique that assigns secret ratings to prospective renters using a proprietary algorithm);[2] *In the Matter of Whatsapp, Inc.,* Complaint, Request for Investigation, Injunction, and Other Relief (Aug. 29, 2016) (challenging Facebook's plan to transfer Whatsapp data to Facebook).[3] EPIC has focused specific attention to the problem of data breaches caused by the failure to secure user data. *See, e.g.*, EPIC, *LinkedIn Breach Leads to 6.5 Million Stolen Passwords* (June 7, 2012).[4] And this week the *New York Times* reported that EPIC's 2019 complaint to the Federal Trade Commission triggered changes in Zoom, the video conferencing service on which much of the nation now depends. Natasha Singer, et al., *Zoom Rushes to Improve Privacy for Consumers Flooding Its Service,* N.Y. Times (Apr. 8, 2020).[5]

For the foregoing reasons, EPIC respectfully requests that this Court grant leave to participate as

---

[2] *Available at* https://epic.org/2020/02/epic-files-complaint-with-ftc-1.html.

[3] *Available at* https://epic.org/privacy/ftc/whatsapp/EPIC-CDD-FTC-WhatsApp-Complaint-2016.pdf.

[4] https://epic.org/2012/06/linkedin-breach-leads-to-65-mi.html.

[5] https://www.nytimes.com/2020/04/08/business/zoom-video-privacy-security-coronavirus.html.

amicus curiae and to file the accompanying *amicus curiae* brief.

Respectfully submitted,

MARC ROTENBERG
ALAN BUTLER
MEGAN IORIO
ELECTRONIC PRIVACY
INFORMATION CENTER (EPIC)
1519 New Hampshire
Avenue NW
Washington, DC 20036
(202) 483-1140
(202) 483-1248 (fax)
rotenberg@epic.org

April 13, 2020

TABLE OF CONTENTS

TABLE OF AUTHORITIES

STATUTES

OTHER AUTHORITIES

INTEREST OF THE *AMICUS CURIAE*

The Electronic Privacy Information Center (EPIC) is a public interest research center in Washington, D.C.[1] EPIC was established in 1994 to focus public attention on emerging civil liberties issues, to promote government transparency, and to protect privacy, the First Amendment, and other constitutional values.

EPIC has filed several *amicus* briefs in this Court concerning consumer privacy. *See, e.g.*, Brief for EPIC et al. as *Amici Curiae* Supporting Petitioners, *Barr v. Am. Ass. of Political Consultants*, No. 19-631 (U.S. filed Nov. 14, 2019) (arguing that the Telephone Consumer Protection Act is constitutional); Brief for EPIC as *Amicus Curiae* Supporting Respondents, *PDR Network v. Carlton & Harris Chiropractic*, 139 S. Ct. 2051 (2019) (No. 17-1705) (arguing that TCPA defendants should not be able to challenge FCC interpretations of the TCPA outside the review process Congress established); Brief for EPIC et al. as *Amici Curiae* Supporting Respondent, *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540 (2016) (No. 13-1339) (arguing that violation of statutory privacy rights confers Article III standing); Brief of EPIC et al. as *Amici Curiae* Supporting Petitioner, *Maracich v. Spears,* 570 U.S. 48 (2013) (No. 12-25) (arguing that the scope of the litigation exception

---

[1] In accordance with Rule 37.2(a), both parties were notified of the intent to file this amicus ten days prior to the filing date. Petitioner consents to the filing of this brief, but respondent has not replied. EPIC motions for leave to file this brief under Rule 37.2(b). In accordance with Rule 37.6, the undersigned states that no monetary contributions were made for the preparation or submission of this brief, and this brief was not authored, in whole or in part, by counsel for a party.

to the Driver's Privacy Protection Act should be narrow); Brief for EPIC et al. as *Amici Curiae* Supporting Petitioners, *Sorrell v. IMS Health*, 564 U.S. 552 (2011) (No. 10-779) (arguing that a Vermont law restricting use of prescriber-identifying data protected patient privacy); Brief for EPIC as *Amicus Curiae* Supporting Petitioners, *Reno v. Condon*, 528 U.S. 141 (2000) (No. 98-1464) (arguing that the Driver Privacy Protection Act was consistent with constitutional principles of federalism).

EPIC has a unique interest in this case because the lower court's decision threatens the privacy interests of internet users, who are not represented by either of the parties in this case. EPIC participated as *amicus curiae* in the Ninth Circuit case below. Brief for EPIC as *Amicus Curiae* in Support of Appellant, *hiQ Labs, Inc. v. LinkedIn Corp.*, 938 F.3d 985 (9th Cir. 2019) (No. 17-16783).

EPIC has led the effort to establish consumer privacy safeguards in the United States. For example, EPIC's 2009 Federal Trade Commission complaint concerning Facebook's privacy practices helped establish the agency's historic consent order. Fed. Trade. Comm'n, *Facebook Settles FTC Charges That It Deceived Consumers by Failing to Keep Privacy Promises* (Nov. 29, 2011)[2] ("Facebook's privacy practices were the subject of complaints filed with the FTC by the Electronic Privacy Information Center and a coalition of consumer groups.") EPIC has filed numerous other complaints at the FTC against companies that do not adequately protect user data. *See, e.g., In the Matter of Airbnb, Inc.,* Complaint and Request for Investigation,

---

[2] https://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep.

Injunction, and Other Relief (Feb. 26, 2020) (challenging Airbnb's deployment of a "risk assessment" technique that assigns secret ratings to prospective renters using a proprietary algorithm);[3] *In the Matter of Whatsapp, Inc.,* Complaint, Request for Investigation, Injunction, and Other Relief (Aug. 29, 2016) (challenging Facebook's plan to transfer Whatsapp data to Facebook).[4] EPIC has focused specific attention to the problem of data breaches caused by the failure to secure user data. *See, e.g.*, EPIC, *LinkedIn Breach Leads to 6.5 Million Stolen Passwords* (June 7, 2012).[5] And this week the *New York Times* reported that EPIC's 2019 complaint to the Federal Trade Commission triggered changes in Zoom, the video conferencing service on which much of the nation now depends. Natasha Singer, et al., *Zoom Rushes to Improve Privacy for Consumers Flooding Its Service,* N.Y. Times (Apr. 8, 2020).[6]

---

[3] *Available at* https://epic.org/2020/02/epic-files-complaint-with-ftc-1.html.

[4] *Available at* https://epic.org/privacy/ftc/whatsapp/EPIC-CDD-FTC-WhatsApp-Complaint-2016.pdf.

[5] https://epic.org/2012/06/linkedin-breach-leads-to-65-mi.html.

[6] https://www.nytimes.com/2020/04/08/business/zoom-video-privacy-security-coronavirus.html.

SUMMARY OF THE ARGUMENT

Earlier this year, the *New York Times* reported that Clearview AI had scraped over three billion photos from web pages to create an unprecedented face surveillance tool. The public was outraged. So too were the companies whose user data was scraped. Companies have explicit terms that restrict the collection and subsequent use of user data obtained from the service. Several of these companies sought to enforce these terms against Clearview. But under the rule adopted by the Ninth Circuit in this case, the companies may be *required* to allow Clearview AI and other third parties to scrape users' data and use the data for their own purposes, regardless of the terms that users of the service are otherwise required to follow. That cannot be the right outcome. The lower court erred in granting an injunction prohibiting LinkedIn from protecting user data.

Clearview AI, like hiQ, is not the first company to use scraped web data in an unexpected and unethical way. Scraping websites and social media profiles is a cheap and easy way to obtain personal data for commercial purposes. But users do not expect that their data will be collected, analyzed, and used by third parties, particularly if they themselves are subject to restrictions on how they may use the data they access. A Facebook user who adds a public profile picture does not give license to a third party to use their photo to create a biometric profile of their face, or to use their name or likeness for commercial value without their consent. Restatement (Second) of Torts § 652C (Appropriation of Name or Likeness); *see, e.g.,* N.Y. Civ. Rights Law § 50. Right of privacy. Notably, the

appropriation tort applies to personal information that is generally available to the public.

Companies that collect data directly from users are required by law to protect the data. Companies are bound by the terms of their user agreements, privacy policies, and other representations, which give users the right to restrict retention, use, and distribution of their personal information. This system of user rights and company obligations forms the basis of modern privacy law. But absent a comprehensive federal data protection law, third-party web scrapers are not obligated to protect the user data of most Americans. Users may never even know that a third party has collected or used their data. Companies are thus in the best position to protect user data and have a responsibility to do so. The lower court's decision makes it impossible for companies to fulfil their responsibility and sets a dangerous precedent that could threaten the privacy of user data.

ARGUMENT

I. Limiting third party access to personal data is consistent with the principles of modern privacy law.

Modern privacy law recognizes that individuals have the right to control their personal data held by others. This right aligns the expectations of individuals with the intended use of their information. Individuals provide personal data for specific purposes and do not expect that their data will be used for other purposes. This includes personal data, which, viewable to the general public. But users do not expect that their data will be used to surveille them, or to make individualistic predictions about their future behavior.

Consumers may not have even chosen to make the information public—and may not know it is generally viewable by the public. Companies must be able to limit unexpected third-party uses of their users' data.

The central purpose of modern privacy law is to recognize individual user rights to control the collection, use, retention, and disclosure of their personal information, and to create a corresponding set of obligations on data collectors. The modern approach to privacy law was set out in the "Fair Information Practices," first developed in the United States in the 1970s by the Department of Health, Education, and Welfare. Marc Rotenberg, *Fair Information Practices and the Architecture of Privacy*, 2001 Stan. Tech. L. Rev. 1, ¶¶ 43, 44. Congress has implemented the Fair Information Practices in several different data privacy statutes, including the Privacy Act, 5 U.S.C. § 552a(e), the Cable Act, 47 U.S.C. § 551, and the Video Privacy Protection Act, 18 U.S.C. § 2710.

Personal data should be relevant to the purposes for which they are to be used. *See* 5 U.S.C. § 552a(e)(5); 47 U.S.C. § 551(b). And the purposes for which personal data are collected should be specified at the time of data collection, with subsequent use limited to the fulfillment of those purposes. *See* 5 U.S.C. § 552a(b) ("Conditions of Disclosure"); 47 U.S.C. § 551(c) ("Protection of subscriber privacy - Disclosure of personally identifiable information").

Consumers provide information to companies for specific purposes. For instance, users create LinkedIn profiles to showcase their education, skills, and experience to colleagues, potential professional contacts, and potential future employers. People use the services of other companies for other specific

purposes: Twitter, to engage in a public conversation; YouTube, to share videos; and Venmo, to make online payments.

Consumers also make some information about themselves viewable to the general public for specific purposes. LinkedIn users create public profiles so that people who are not currently in their LinkedIn network can find them and view parts of their online resume. LinkedIn, *Public Profile Visibility* (2020).[7] LinkedIn represents that this public profile will be used for particular purposes: search engine indexing, public profile badges, and on third-party sites that are affiliates with or approved by LinkedIn. *Id*. LinkedIn also allows users to opt-out of certain uses for their public profiles, such as whether third-party applications can use the data. LinkedIn, *Off-LinkedIn Visibility* (2020).[8] LinkedIn users can also prevent the company from using profile updates to send alerts to their connections. 3ER-427. About 20% of LinkedIn users take advantage of this feature. 3ER-430. The popularity of the feature suggests that users do not want their current employers to be notified when they update their LinkedIn profile, which can be an indication that the employee is looking for a new job.

LinkedIn users do not expect that the photo they provide for their public profile will be used to create a biometric profile of their face, or that their online resume will be used to predict how much time they are likely to stay at their current job. Indeed, the popularity of the "Do Not Broadcast" feature shows that LinkedIn users do not want or expect companies like

---

[7] https://www.linkedin.com/help/linkedin/answer/83/linkedin-public-profile-visibility?lang=en.

[8] https://www.linkedin.com/help/linkedin/answer/79854.

hiQ to use their LinkedIn data to inform their current employers that they may leave their job within a certain timeframe.

Predictive employment analytics pose several significant privacy risks. Data scientist Cathy O'Neil has stated that "throughout the tech industry, many companies are busy trying to optimize their white-collar workers by looking at the patterns of their communications," and these systems "have the potential to become true [weapons of math destruction]. They can misinterpret people, and punish them, without any proof that their scores correlate to the quality of their work." Cathy O'Neil, *Weapons of Math Destruction*, 133 (2016). The U.S. Equal Opportunity Employment Commission has warned employers "to not simply 'trust the math'" with these types of employee algorithms, "as the math in this case has been referred to, by at least one mathematician/data scientist, as an 'opinion formalized in code.'" Written Testimony of Kelly Trindel, PhD, Chief Analyst, Office of Research, Info. & Planning, Equal Emp't Opportunity Comm'n (Oct. 13, 2016) (describing specifically hiQ's data practices).[9] Because the results of these algorithms can significantly impair crucial life opportunities, such as whether we are "good credit risks, desirable employees, reliable tenants, valuable customers—or deadbeats, shirkers, menaces, and 'wastes of time,'" Professors Danielle Keats Citron and Frank A. Pasquale call for greater transparency and oversight of predictive algorithms. Danielle Keats Citron & Frank A. Pasquale,

---

[9] https://www.americanbar.org/content/dam/aba/events/labor_law/2017/03/err/papers/steele_paper.authcheckdam.pdf.

The Scored Society: Due Process for Automated Predictions, 89 Wash. L. Rev. 1, 1 (2014).

Scraping public data from one company's website and combining it with data from other sources can also result in unexpected and harmful consequences. Professor Anita L. Allen has observed that individuals in the Big Data world are not well positioned to anticipate how their data will be combined by third parties "to reveal otherwise unascertained patterns, links, behaviors, trends, identities, and practical knowledge." Anita L. Allen, *Protecting One's Own Privacy in a Big Data Economy*, 130 Harv. L. Rev. F. 71, 71 (2016).[10] For example, while many Twitter users associate their real identities with their Twitter content, many also use Twitter under pseudonyms. A third party could attempt to identify these anonymous Twitter users by trying to match their Twitter information with data obtained elsewhere. Twitter is aware that of this potential use of Twitter user data and prohibits developers from attempting it. Twitter, *Developer Terms* (2020).[11]

Additionally, users often do not have a choice whether their personal information is "public"—and they may not even know that the information is out there for the world to see. First, someone else may have posted the user's data. Second, a user may not be aware that their posts are set to "public." Privacy settings are often difficult to understand and some companies, notably Facebook, frequently change privacy settings to make information more widely available than a user would anticipate. Controlling privacy on

---

[10] https://harvardlawreview.org/2016/12/protecting-ones-own-privacy-in-a-big-data-economy/.

[11] https://developer.twitter.com/en/developer-terms/policy.

Facebook is so complex that the company has a twelve-step tutorial on how to use the settings. Facebook, *Manage Your Privacy* (2020).[12] When Facebook has changed privacy settings in the past, content that users posted that they thought was not generally accessible suddenly became public. In 2009, *amicus* EPIC brought a complaint to the Federal Trade Commission that documented changes in Facebook privacy settings that made user information and content, such as profile pictures, public that users had previously designated as private. *In the Matter of Facebook, Inc.,* Complaint, Request for Investigation, Injunction, and Other Relief (Dec. 17, 2009).[13] The complaint led to a 2011 consent order against Facebook. *In the Matter of Facebook, Inc.,* Consent Order, FTC Docket No. C-4365 (July 27, 2012).[14] But even after the FTC consent order, Facebook continued to publicly expose previously private user content. *See, e.g.,* Alex Hern, *Facebook Is Chipping Away at Privacy—and My Profile Has Been Exposed*, The Guardian (Jun. 29, 2016);[15] Brian Barrett, *Facebook Search Now Finds Public Posts—So Hide Yours*, Wired (Oct. 22, 2015).[16]

Third, a company's error can expose data that the user chose not to make publicly viewable. For instance, in May 2018, Facebook made public the posts

---

[12] https://www.facebook.com/about/basics/manage-your-privacy.

[13] *Available at* https://www.epic.org/privacy/inreface-book/EPIC-FacebookComplaint.pdf.

[14] *Available at* https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookd o.pdf.

[15] https://www.theguardian.com/technology/2016/jun/29/facebook-privacy-secret-profile-exposed.

[16] https://www.wired.com/2015/10/facebook-search-privacy/.

of as many as 14 million users that thought they were only sharing with their friends or a smaller group. Kurt Wagner, *Facebook Says Millions of Users Who Thought They Were Sharing Privately with Their Friends May Have Shared with Everyone Because of a Software Bug*, Vox (Jun. 7, 2018). A few weeks later, Facebook unblocked users who had been previously blocked by other users, allowing the newly unblocked users to view content they should not have been permitted to view. Kurt Wagner, *Facebook's Year of Privacy Mishaps Continues—This Time with a New Software Bug that 'Unblocked' People*, Vox (Jul. 2, 2018).[17]

Companies such as LinkedIn should limit third-party access to user data act in accordance with modern privacy law. An injunction prohibiting such limitations is against the public interest, in particular because the United States lacks a comprehensive federal data privacy law.

II. Internet companies have a responsibility to protect the data of their users from third parties

The United States does not have a comprehensive federal data protection law codifying globally recognized rights to data privacy. While some states, such as California and Illinois, have enacted data protection laws of varying scope, most Americans are not protected by a data privacy statute. In the absence of comprehensive data protection laws, user rights are usually encompassed in agreements between data collectors and users. Companies, as the primary data collectors, are obligated to ensure that user data is collected,

---

[17] https://www.vox.com/2018/7/2/17528220/facebook-software-bug-block-unblock-safety-privacy.

used, disclosed, and retained according to the company's user agreement, privacy policy, user settings, and other representations. But third parties are not bound by these understandings. Thus, absent a comprehensive federal privacy law, companies who are in privity to their users are in the best position to protect their users' privacy by limiting access to user data, such as by prohibiting scraping and requiring access through an application programming interface ("API"). An API can enable companies to limit third-party access and to enforce user privacy protections.

Companies in privity to their users, as the primary collectors of data, must limit the collection, use, disclosure, and retention of personal data in accordance with their user agreements, privacy policies, and other representations. For instance, companies such as LinkedIn and Twitter guarantee that they will stop displaying user data within 24 hours if the user chooses to delete the data from their profile and, if the user deletes their account, the companies will not retain the data beyond a certain date, usually 30 days after the user requests deletion. LinkedIn, *Privacy Policy*, §§ 4.2–4.3 (2020);[18] Twitter, *Privacy Policy*, §§ 1.2, 4.2 (2020).[19] Companies in privity to their users are also required to honor users' choices as to who can view their information. LinkedIn, *User Agreement*, § 2.5 (2020);[20] Twitter, *Privacy Policy*, *supra*, at § 3.1; Facebook, *Data Policy* (2020).[21] Failure to abide by the agreement can result in legal action against the company. *See, e.g.*, Complaint, *Perkins v. LinkedIn Corp.*,

---

[18] https://www.linkedin.com/legal/privacy-policy.

[19] https://twitter.com/en/privacy.

[20] https://www.linkedin.com/legal/user-agreement.

[21] https://www.facebook.com/about/privacy.

53 F. Supp. 3d 1190 (N.D. Cal. 2014) (concerning privacy tort and Wiretap Act claims arising from the "harvesting" of "e-mail addresses from the contact lists" of Plaintiffs' associated accounts); *In re Facebook, Inc., Consumer Privacy User Profile Litigation*, No. 3:2018-md-02843 (N.D. Cal. docketed June 6, 2018) (concerning Facebook's breach of user agreements involving Cambridge Analytica).

But third-party scrapers are not bound by the user agreements of the websites they scrape, nor do they generally provide similar rights to consumers whose data was scraped. For instance, hiQ's privacy policy does not even mention the rights of those whose data is scraped. hiQ Labs, *Privacy Policy, supra*.

Many companies control third-party access to user data by prohibiting scraping and instead requiring access through an API. LinkedIn's user agreement, for example, prohibits data scraping, bypassing access controls, or copying, using, disclosing, or distributing LinkedIn user data without consent. LinkedIn, User Agreement, *supra*, at §§ 8.2(b)–(d). LinkedIn requires third parties to obtain either a LinkedIn user's permission, or LinkedIn's permission, to access user data through their API. LinkedIn, *Permissions* (2020).[22] Even Twitter, whose users generally post publicly viewable data, prohibits scraping user data without Twitter's consent, Twitter, *Terms of Service*, § 4 (2020),[23] and requires developer to seek permission from Twitter to access user data through the API. Twitter, *Developer Terms*, *supra*.

---

[22] https://docs.microsoft.com/en-us/linkedin/shared/authentication/permissions?context=linkedin/consumer/context.

[23] https://twitter.com/en/tos.

Forcing access to a company's data through an API makes it possible for a company to screen developers and monitor their use of user data. Twitter requires that developers disclose "all proposed uses of the Twitter developer platform to verify policy compliance — so you're required to disclose (and update, as applicable) your planned use of the Twitter API and Twitter Content in order to be granted and to maintain access." Twitter, *Developer Terms*, *supra*. Facebook also requires that developers describe how they will use each category of Facebook data they wish to collect. Facebook, *Login Permissions* (2020);[24] Facebook, *Sample App Review Submission for Facebook Login* (2020).[25]

The API also ensures that third parties comply with a user's privacy settings. Twitter, for example, requires third parties to display current versions of Twitter public posts—or to remove them if they are deleted from the company's website. Twitter, *Developer Terms*, *supra*.

Many companies explicitly ban developers from certain unethical and unexpected uses of personal data. Twitter, for instance, prohibits third parties from using Twitter user data "in any way that would be inconsistent with people's reasonable expectations of privacy." *Id*. Twitter's list of prohibited uses includes credit or insurance risk analysis, individual profiling or "psychographical segmentation," facial recognition, and deriving or inferring sensitive information about individual users, such as health, political affiliation,

---

[24] https://developers.facebook.com/docs/apps/review/login-permissions.

[25] https://developers.facebook.com/docs/facebook-login/review/sample-submission.

race, ethnicity, sexual orientation, and off-Twitter identity. Twitter, *More About Restricted Uses of the Twitter APIs* (2020).[26] LinkedIn's API terms of use prohibit data use "that may harm the professional reputation, relationships or professional ecosystem of" LinkedIn users. LinkedIn, *API Terms of Use*, § 3.1(a) (2020).[27] LinkedIn also prohibits data use that "facilitates bias or discriminatory practices" or "facilitates government surveillance." *Id.* at §§ 3.1(q)–(r). Facebook similarly bans using Facebook user data for "tools that are used for surveillance." Facebook, *Facebook Platform Policy*, § 3.1 (2020).[28]

Of course, for these rules to be effective, they must actually be enforced by the companies. The Cambridge Analytica scandal occurred because Facebook did not monitor Cambridge Analytica's collection and use of user data, did not take prompt action to stop the company's access when the misuse was discovered, and did not ensure that the data was deleted. Carole Cadwalladr & Emma Graham-Harrison, *Revealed: 50 million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach*, The Guardian (Mar. 17, 2018).[29] The consensus following Cambridge Analytica is that companies in privity to their users must protect user privacy by, among other things, limiting and monitoring third-party access to user data. And following the recent revelation that an obscure company called Clearview AI scraped billions of images

---

[26] https://developer.twitter.com/en/developer-terms/more-on-restricted-use-cases.

[27] https://legal.linkedin.com/api-terms-of-use.

[28] https://developers.facebook.com/policy.

[29] https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.

from across the internet for a facial recognition system, popular companies have moved to enforce their terms of service through cease-and-desist letters. Unfortunately, the lower court's decision could prevent companies from protecting their users' personal data from scraping by Clearview AI.

III. Clearview AI scraped billions of images from across the internet to make facial recognition profiles of everyday Americans.

In January, the *New York Times* revealed that Clearview AI had scraped over three billion images from millions of websites to create an unprecedented facial recognition tool for law enforcement and private entities. Kashmir Hill, *The Secretive Company That Might End Privacy As We Know It*, N.Y. Times (Jan. 18, 2020).[30] The company scraped images from Facebook, YouTube, Twitter, Instagram, and even Venmo, an online payment application. *Id.* The images were used to create biometric templates of each identifiable face. *Id.* When a user uploads a photo to search Clearview's system, the program returns all related scraped photos, along with links to the sites from which the images were taken. *Id.* All of the images scraped by Clearview were so-called "public" images—that is, someone at some point chose to make the image viewable by any human, the company made the image generally viewable by default, or some bug in the company's software made the image temporarily available to all.

---

[30] https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.

Like hiQ's conduct in the case below, Clearview AI raised significant privacy concerns precisely because the company scraped personal data from website. Previously, most facial recognition software could only identify individuals from a limited database of faces, such as prior arrests or previous contacts. But because nearly every adult—and a large number of children—have several images of themselves, linked to their identities, somewhere on the internet, Clearview AI can potentially identify nearly *anyone*, including children. Kashmir Hill & Gabriel J.X. Dance, *Clearview's Facial Recognition App Is Identifying Child Victims of Abuse*, N.Y. Times (Feb. 7, 2020).[31]

Also, like hiQ, Clearview made personal data available to thousands of entities. As of February, more than 2,200 institutions had run nearly 500,000 searches on Clearview. Caroline Haskins, et al., *Clearview's Facial Recognition App Has Been Used by the Justice Department, ICE, Macy's, Walmart, and the NBA*, Buzzfeed News (Feb. 27, 2020).[32] Federal, state, and local law enforcement agencies across the country have used the facial recognition tool, along with more than 200 private companies and 50 educational institutions. *Id.* Clearview has disclosed personal data to big box stores such as Walmart, department stores such as Macy's, and entertainment facilities including Madison Square Garden, as well as casinos, fitness centers, and financial institutions. *Id.* In addition, Clearview has appealed to private investigators and security firms. *Id.*

---

[31] https://www.nytimes.com/2020/02/07/business/clearview-facial-recognition-child-sexual-abuse.html.

[32] https://www.buzzfeednews.com/article/ryanmac/clearview-ai-fbi-ice-global-law-enforcement.

Once a third party has possession of scraped data, they may disclose it to individuals who are not accountable to the data subject. Clearview has made its facial recognition tool available to friends of the founders, political allies, and potential investors. Ryan Mac, et al., *Secret Users of Clearview AI's Facial Recognition Dragnet Included a Former Trump Staffer, a Troll, And Conservative Think Tanks*, Buzzfeed News (Mar. 11, 2020).[33] Some of these users have been reported to casually use the facial recognition tool to identify new acquaintances. *Id*. Some have expressed interest in using the technology for more nefarious purposes, including opposition research. Hill, *The Secretive Company That Might End Privacy As We Know It*, *supra*.

Clearview's reported plans for expansion pose particularly acute privacy risks. According to a Buzzfeed News investigation, the company is developing surveillance cameras and augmented reality glasses to use in conjunction with the Clearview facial recognition database. Caroline Haskins, et al., *The Facial Recognition Company That Scraped Facebook and Instagram Photos Is Developing Surveillance Cameras*, Buzzfeed News (Mar. 2, 2020).[34] These tools would allow users to identify individuals in real-time, effectively ending Americans' ability to be anonymous in public. The company also has plans to expand to at least 22 countries outside the United States, some of which are ruled by authoritarian regimes with dismal

---

[33] https://www.buzzfeednews.com/article/ryanmac/clearview-ai-trump-investors-friend-facial-recognition.

[34] https://www.buzzfeednews.com/article/carolinehaskins1/clearview-facial-recognition-insight-camera-glasses.

human rights records. Caroline Haskins, et al., *Clearview AI Wants to Sell Its Facial Recognition Software to Authoritarian Regimes Around the World*, Buzzfeed News (Feb. 5, 2020).[35]

Like hiQ, Clearview limits consumers' ability to remove their data from the company's system. Clearview's privacy policy states that consumers have certain rights to control their data—but notes that the company will only honor requests to exercise these rights "as required under applicable data protection rules." Clearview AI, *Privacy Policy* (2020).[36] California residents have rights to control their data under the state's new Consumer Privacy Protection Act, and Clearview allows California residents to exercise their rights—as long as they provide the company with a photo of themselves. Clearview AI, *Privacy Request Forms* (2020).[37] For all other Americans, however, Clearview intends to continue scraping images and retaining those it has already acquired—even if the consumer has deleted or limited access to the original image. Clearview will only remove an image from search results if the consumer has removed the image from the site of origin *and* submitted a form with the image's previous URL. Clearview AI, *Deindex Request* (2020).[38] But consumers rarely have control over every image of them on the internet—some are posted by friends, family, or other third parties. Nor do they know of every image of them that exists online. Even

---

[35] https://www.buzzfeednews.com/article/carolinehaskins1/clearview-ai-facial-recognition-authoritarian-regimes-22.

[36] https://staticfiles.clearview.ai/privacy_policy.html.

[37] https://clearview.ai/privacy/requests.

[38] https://clearview.ai/privacy/deindex.

for images controlled by the consumer, the company forces the consumer to choose between making their image viewable by humans in the general public and having their image used in a surveillance system—a choice users should not have to make. In contrast, search engines like Google recognize that not every person wants publicly available images to be included in Google searches, and allows websites to prevent image indexing. Google, *Prevent Images on Your Page from Appearing in Search Results* (2020).[39]

Just as LinkedIn has done with hiQ, it and several other companies have demanded that Clearview AI stop scraping their users' data and delete the data that Clearview AI has already scraped. Twitter sent the company a cease-and-desist letter and pointed to its developer policy, which prohibits using Twitter users' data for facial recognition. Kashmir Hill, *Twitter Tells Facial Recognition Trailblazer to Stop Using Site's Photos*, N.Y. Times (Jan. 22, 2020);[40] Twitter, *More About Restricted Uses of the Twitter APIs* (2020).[41] Google, YouTube, Venmo, and LinkedIn also sent Clearview cease-and-desist letters, pointing to their terms of service, which prohibit or limit scraping user data. Gisela Perez & Hilary Cook, *Google, YouTube, Venmo and LinkedIn Send Cease-and-Desist Letters to Facial Recognition App that Helps Law*

---

[39] https://support.google.com/webmasters/answer/35308.

[40] https://www.nytimes.com/2020/01/22/technology/clearview-ai-twitter-letter.html.

[41] https://developer.twitter.com/en/developer-terms/more-on-restricted-use-cases.

Enforcement, CBS News (Feb. 5, 2020).[42] Facebook sent a cease-and-desist letter as well demanding that the company stop using information from Facebook and Instagram. Haskins, et al., *supra*. But many of the news stories covering the Clearview scandal noted that the Ninth Circuit's decision prevents companies in privity with their users from taking legal action to protect their users' privacy. Steven Melendez, *Facebook Orders Creepy AI Firm to Stop Scraping Your Instagram Photos,* Fast Company (Feb. 6, 2020);[43] Louise Matsakis, *Scraping the Web Is a Powerful Tool. Clearview AI Abused It*, Wired (Jan. 25, 2020);[44] Hill, *Twitter Tells Facial Recognition Trailblazer to Stop Using Site's Photos*, *supra*.

Government officials also expressed alarm about Clearview's facial recognition system and its use of scraped data. The chairwoman and ranking member of the House Committee on Science, Space & Technology have demanded that Clearview explain in detail where and how the company collects its data. Letter from Reps. Eddie Bernice Johnson & Frank D. Lucas to Hoan Ton-That, Chief Exec. Officer, Clearview AI (Mar. 3, 2020).[45] In his letter seeking answers from the company, Senator Ed Markey distinguished Clearview AI from other facial recognition tools because "it

---

[42] https://www.cbsnews.com/news/clearview-ai-google-youtube-send-cease-and-desist-letter-to-facial-recognition-app/.

[43] https://www.fastcompany.com/90461077/facebook-joins-fellow-tech-companies-in-publicly-opposing-a-controversial-face-recognition-firm.

[44] https://www.wired.com/story/clearview-ai-scraping-web/.

[45] https://science.house.gov/imo/media/doc/3.03.2020%20Letter%20to%20Clearview%20AI.pdf.

scrapes billions of photos from social media sites rather than using relatively limited sets of photos from existing government databases," resulting in an image database of "unprecedented scope." Letter from Sen. Edward J. Markey to Hoan Ton-That, Chief Exec. Officer, Clearview AI (Mar. 3, 2020).[46] Senator Ron Wyden declared that "Americans have a right to know whether their personal photos are secretly being sucked into a private facial recognition database." Sen. Rob Wyden (@RonWyden), *Twitter* (Jan. 19, 2020, 8:25 AM).[47] New Jersey's Attorney General Gurbir Grewal told all law enforcement agencies in the state to stop using Clearview's system and began an inquiry into how state agencies have used the system. Kashmir Hill, *New Jersey Bars Police from Using Clearview Facial Recognition App*, N.Y. Times (Jan. 24, 2020).[48] Grewal said that he opposes "the wide-scale collection of biometric information and the use of it without proper safeguards." Perez & Cook, *supra*.

Clearview has been sued under state data protection laws, such as the Illinois Biometric Privacy Act. Class Action Complaint, *Mutnick v. Clearview AI, Inc.*, No. 1:20-cv-00512 (N.D. Ill. filed Jan. 22, 2020). But most states do not have strong data protection laws, and there is no comprehensive federal privacy law in the United States. Because the Ninth Circuit's decision in this case prevents companies from protecting

---

[46] https://www.markey.senate.gov/imo/media/doc/Markey%20Letter%20-%20Clearview%20II%203.3.20.pdf.

[47] https://twitter.com/RonWyden/status/1218887171911880704.

[48] https://www.nytimes.com/2020/01/24/technology/clearview-ai-new-jersey.html.

their users' data from scrapers like Clearview, the privacy of a broad majority of Americans remains at great risk.

Clearview and hiQ are not the first companies to make unexpected and unethical use of scraped user data—and will not be the last. For instance, in 2017, researchers at Stanford claimed to have developed a tool that could predict whether a person was gay from their photo. Yilun Wang & Michal Kosinski, *Deep Neural Networks are More Accurate than Humans at Detecting Sexual Orientation from Facial Images*, 114 J. Personality & Soc. Psychol. 246 (2018). The researchers scraped over 130,000 photos from so-called "public" profiles on a U.S. dating website, along with the gender of the potential partners flagged by users. *Id.* at 248. The research was condemned by leading LGBTQ+ rights groups GLAAD and the Human Rights Campaign, who warned that such a tool "could serve as a weapon to harm both heterosexuals who are inaccurately outed, as well as gay and lesbian people who are in situations where coming out is dangerous." Drew Anderson, *GLAAD and HRC Call on Stanford University & Responsible Media to Debunk Dangerous & Flawed Report Claiming to Identify LGBTQ People Through Facial Recognition Technology*, GLAAD (Sep. 8, 2017).[49]

These examples show how personal data can be used in unexpected and unethical ways. Companies in privity with their users must be able to protect users by limiting third-party access to personal data. The

---

[49] https://www.glaad.org/blog/glaad-and-hrc-call-stanford-university-responsible-media-debunk-dangerous-flawed-report.

lower court's decision prevents this and must be reversed.

CONCLUSION

For the above reasons, *amicus* EPIC respectfully asks this Court to grant the petition for a writ of certiorari.

Respectfully submitted,

MARC ROTENBERG
ALAN BUTLER
MEGAN IORIO
ELECTRONIC PRIVACY
INFORMATION CENTER (EPIC)
1519 New Hampshire
Avenue NW
Washington, DC 20036
(202) 483-1140
(202) 483-1248 (fax)
rotenberg@epic.org

April 13, 2020