No. 17-16783

IN THE UNITED STATES COURT OF APPEALS FOR THE NINTH CIRCUIT

HIQ LABS, INC.

Plaintiff-Appellee,

v.

LINKEDIN CORPORATION,

Defendant-Appellant.

On Appeal from the United States District Court
for the Northern District of California
Case No. 3:17-cv-03301-EMC
The Honorable Edward M. Chen, Presiding

Brief of Amicus Curiae Electronic Privacy Information Center (EPIC) in Support of Neither Party Urging Reversal

Marc Rotenberg
Alan Butler
Electronic Privacy Information Center
1718 Connecticut Ave. NW
Suite 200
Washington, DC 20009
(202) 483-1140

Counsel for Amicus Curiae

October 10, 2017

CORPORATE DISCLOSURE STATEMENT

Pursuant to Federal Rules of Appellate Procedure 26.1 and 29(c), Amicus Curiae Electronic Privacy Information Center ("EPIC") is a District of Columbia corporation with no parent corporation. No publicly held company owns 10% or more of EPIC stock.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

OTHER AUTHORITIES

INTEREST OF THE AMICUS[1]

The Electronic Privacy Information Center ("EPIC")[2] is a public interest research center in Washington, D.C., established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and other constitutional values.

EPIC routinely participates as *amicus curiae* in cases concerning consumer privacy before the United States Supreme Court and federal circuit courts, including the United States Court of Appeals for the Ninth Circuit. *See, e.g., Smith v. Facebook, Inc.*, No. 17-16206 (9th Cir. filed Sept. 25, 2017) (arguing that Facebook users do not consent to Facebook's collection of medical data from third-party websites); *In re Nickelodeon Consumer Privacy Litig.*, 827 F.3d 262 (3rd Cir. 2016) (arguing that unique persistent identifiers are "personally identifiable information" under the Video Privacy Protection Act); *Fraley v. Batman*, 638 Fed. App'x 594 (9th Cir. 2016) (arguing that Facebook's "Sponsored Stories" settlement was not fair or sufficient for class members); *Joffe v. Google, Inc.*, 746 F.3d 920 (9th Cir. 2013) (arguing that interception of Wi-Fi communications from home networks violated the federal Wiretap Act).

---

[1] Both parties consent to the filing of this brief. In accordance with Rule 29, the undersigned states that no monetary contributions were made for the preparation or submission of this brief. Counsel for a party did not author this brief, in whole or in part.

[2] EPIC Appellate Advocacy Fellow Natasha Babazadeh contributed to this brief.

ARGUMENT

This is a case between two companies whose businesses are built around the collection and use of personal data. One company has a direct relationship with individuals and a fiduciary obligation to limit the use and disclosure of the data obtained. The other company has no relationship with individuals, other than to acquire their personal data and use for whatever purpose may generate commercial value. The practices of both companies implicate privacy interests. But in the matter before this Court, it is the practices of hiQ Labs that are at odds with the interests of individuals. And in this Court's consideration of the mandatory injunction issued by the lower court, the privacy interests of those who provide personal data should be paramount.

Personal data is central to this case even though users are not represented in this proceeding. Regrettably, the lower court discounted the privacy interests of users and required LinkedIn to make the personal data of LinkedIn users available to data aggregators for whatever purpose they wish. That cannot be correct. LinkedIn users expect that the personal data they provide will be used to advance their careers, not acquired by an unaccountable third party to assess their "flight risk." The lower court erred when it mandated that personal data be made available to hiQ Labs. That is contrary to the "public interest" determination for the issuance of an injunction. *Lair v. Bullock*, 697 F.3d 1200 (9th Cir. 2012).

LinkedIn users provide personal data to LinkedIn for a particular purpose. The company describes itself as "the world's largest professional network" whose mission is to "connect the world's professionals to make them more productive and successful." LinkedIn, *About Us* (2017).[3] Users reasonably expect that the personal information they provide will enhance their career prospects and facilitate professional relationships. That is the bargain between the users and the company, set out in the User Agreement, which states that "[i]f you reside in the United States, you are entering into the User Agreement with LinkedIn Corporation, who will be responsible for your personal data provided to, or collected by or for, our Services." LinkedIn, *Privacy Policy* (2017).[4] LinkedIn further states we "will get your consent if we want to give third parties the right to publish your posts beyond the Service." *Id*. By issuing a mandatory injunction compelling the release of user data to third parties, the lower court has undermined the fiduciary relationship established between LinkedIn and its users.

I. LinkedIn users create profiles and provide personal information for professional networking purposes with the understanding that LinkedIn will protect their data as required by law.

LinkedIn is a website that provides users with business and professional networking services. Their main objective is "to connect the world's professionals

[3] https://press.linkedin.com/about-linkedin?trk=uno-reg-guest-home-about.
[4] https://www.linkedin.com/legal/privacy-policy.

to allow them to be more productive and successful . . . to promote economic opportunity for members by enabling [them] and millions of other professionals to meet, exchange ideas, learn, and find opportunities or employees, work, and make decisions in a network of *trusted* relationships." LinkedIn, *User Agreement* (2017).[5] LinkedIn users can create a profile, list their work experience, education and training, skills, and post professional photos. *Id*. LinkedIn was "developed specifically for the purpose of professional networking, job searching and personal or commercial branding." Erin Stashin, *LinkedIn: A Short Historical Review* (2014).[6]

A LinkedIn profile is important for job applicants:

> Any individual who is not on LinkedIn in 2016 is akin to a small business that was not in the yellow pages, circa 1980. It's suicide. Imagine this: what if you showed up for a job interview in the 1980s or 19990s and refused to produce a resume? That's how decision makers and employers will feel about you if you are not on LinkedIn in 2016.

Laurence Bradford, *11 Reasons Why You Need to be on LinkedIn as an Aspiring Techie*, Learn to Code With Me (Dec. 16, 2015).[7]

hiQ Labs has a very different purpose. According to the company, "[t]here is more information about your employees outside the walls of your organization

---

[5] https://www.linkedin.com/legal/user-agreement.
[6] http://www.tiki-toki.com/timeline/entry/347471/Linkedin-A-Short-Historical-Review/.
[7] https://learntocodewith.me/posts/reasons-to-use-linkedin/.

than inside it." hiQ Labs (2017).[8] hiQ Labs explains that it "provides flight risks and skill footprints of enterprise organizations, allowing HR teams to make better, more reliable people decisions." *Id*. The company claims that it can determine "flight risk" with the "Keeper" tool, which offers "predictive attrition insights about an organization's employees based on publicly available data." hiQ Labs, *Keeper* (2017).[9]

A. LinkedIn users provide personal data for professional networking purposes and do not expect that their data will be acquired and monetized by unknown third-parties.

Users join LinkedIn for a specific purpose: to expand their professional network. They post their resumes, join work-related groups, and participate in discussions on topics of interest. Megan Lacombe, *5 Reasons Why You Should Create a LinkedIn Account*, Liberty Staffing Services (Apr. 6, 2017).[10] Users who join LinkedIn provide detailed personal information to the company, and they reasonably expect that LinkedIn will uphold its end of the bargain by protecting their data from unauthorized disclosure and misuse. If LinkedIn fails to do so, the company can expect that users will take legal action to protect their rights. *See, e.g.*, *Perkins v. LinkedIn Corp.*, 53 F. Supp. 3d 1190 (N.D. Cal. 2014) (concerning

[8] https://www.hiqlabs.com/.
[9] https://www.hiqlabs.com/new-keeper.
[10] http://www.libertystaffing.ca/blog/5-reasons-why-you-should-create-a-linkedin-account.

privacy tort and Wiretap Act claims arising from the "harvesting" of "e-mail addresses from the contact lists" of Plaintiffs' associated accounts). A user's LinkedIn profile is configured specifically to limit access to the personal data that is not necessary to promote their professional goals. If any third-party company could scrape, aggregate, and monetize users' data for a different purpose, it would undermine the core premise of the User Agreement.

A user's profile is a way to showcase work experience, achievements and recommendations from clients or colleagues. LinkedIn, *LinkedIn Profile – Overview* (2017).[11] The profile also provides a way for colleagues or potential employers to contact the user regarding job opportunities. LinkedIn, *Building Your Professional Network* (2017).[12] It is important for users to not only see the colleagues that they are directly "connected" with, but also to be exposed to the "extended network" of professionals connected to their colleagues. LinkedIn, *Connections Overview* (2017).[13]

A LinkedIn profile may contain a wide range of information about the user, and some users choose to make limited profile data searchable or accessible by those who are not within their professional network. First and foremost, a LinkedIn

[11] https://www.linkedin.com/help/linkedin/answer/15493.
[12] https://www.linkedin.com/help/linkedin/answer/348/building-your-professional-network.
[13] https://www.linkedin.com/help/linkedin/answer/15495/connections-overview.

profile contains the users' contact information—name, e-mail, phone number, and physical address—which is only visible to "1st-degree connections" and members with whom the user has directly communicated. LinkedIn, *What People Can See On Your Profile* (2017).[14] Other personal details, such as birthdate, are specifically controllable by the user (who may not want to share that information with their professional network). LinkedIn, *Adjusting Your Birthday Privacy Settings* (2017).[15] In contrast, more generic contact information such as a user's "webpage, blog URL or Twitter handle may be visible to all members." *Id*. But a LinkedIn profile contains more than just contact information.

LinkedIn also collects personal data from users who post information to the site, including responses to surveys and invitations. LinkedIn, *Visibility of Posts and Links You Share* (2017).[16] A user can also choose to import contacts from their address book in order to make connections with professional colleagues. LinkedIn, *Syncing Contacts from Other Address Books and Sources* (2017). LinkedIn represents that this data is transferred securely, will not be shared "with anyone," and that the company will not "sell your personal data." LinkedIn, *Privacy of Your*

[14] https://www.linkedin.com/help/linkedin/answer/77.
[15] https://www.linkedin.com/help/linkedin/answer/84140.
[16] https://www.linkedin.com/help/linkedin/answer/431.

Information in LinkedIn Contacts (2017).[17] None of this information is "publicly available," nor should it be.

LinkedIn has implemented safeguards to protect users against harassment. LinkedIn, *Harassment or Safety Concern* (2017).[18] These threats are a reality that many users, especially women, confront on a daily basis. *See* Nina Bahadur, *It's 2017, and Women Are Still Being Harassed on LinkedIn*, Mic (Apr. 28, 2017). For example, some users who post a professional photo only want the photo to be viewable by others within their network. LinkedIn, *Settings for Profile Photo Visibility* (2017). Users who are trying to prevent harassment may limit who can send them "invitations" or may directly block other users. LinkedIn, *Controlling Who Can Send You Invitations* (2017).[19] Obviously, these protections would be undermined by third party aggregators who collect users' profile data not subject to access restrictions.

B. The existence of a "public profile," accessible to other LinkedIn Users and accessible to search engines, is not a license for use by hiQ.

The "public profile" is a limited profile that a LinkedIn user may choose to make available to search engines and certain third-party applications. LinkedIn

[17] https://www.linkedin.com/help/linkedin/answer/45006/privacy-of-your-information-in-linkedin-contacts.
[18] https://www.linkedin.com/help/linkedin/answer/42605/harassment-or-safety-concern.
[19] https://www.linkedin.com/help/linkedin/answer/70.

represents that the public profile "appears when people search for you using a public search engine like Google, Yahoo!, Bing, DuckDuckGo, etc." LinkedIn, *LinkedIn Public Profile Visibility* (2017). Some users choose not to make their profile visible to these search engines. *Id*. This public profile serves an important purpose for some users: to allow colleagues, clients, and/or potential employers to locate their digital resume and make a professional connection even if they are not subscribed to LinkedIn. The purpose of the public profile is not to enable data analytics companies to scrape, aggregate, and monetize user data.

LinkedIn users also have the ability to change their profiles and to limit the personal data that is available on their public profile. Changes can reflect new employment, skills, awards, and so forth. The user retains the choice of whether to broadcast these changes to their network, which may also include their employer or coworkers. 3ER-427. The "Do Not Broadcast" feature allows a user to control when changes are broadcasted to the user's network. 3ER-427. If the user selects "Do Not Broadcast," their connections are not notified of the changes. 3ER-427. Many users do not want their employers, colleagues, or others to be aware of every change that they make to their profile. As a result, the "Do Not Broadcast" feature is very popular. Over 50 million LinkedIn users, and approximately 20% of the 142 million users who updated their profile information this last year, opted to use the privacy feature. 3ER-430.

Companies such as hiQ Labs that scrape profile data undermine the privacy preferences of LinkedIn users. The tracking of user profile edits negates the user's "Do Not Broadcast" choices. The lower court failed to recognize that a mandatory injunction prohibiting LinkedIn from protecting user profile information would directly harm users' interests. The court also failed to understand the purpose of search engine access to LinkedIn public profiles or to recognize that users retained the ability to limit such access if they choose. The interests of hiQ Labs are not necessarily aligned with the interests of LinkedIn users, and LinkedIn users have no ability to limit hiQ Labs use of their personal data.

For example, under LinkedIn's Privacy Policy, if a user decides to delete an account, LinkedIn promises that "personal data will generally stop being visible to others within 24 hours" and to "delete closed account information within 30 days of account closure." LinkedIn, *Privacy Policy*. LinkedIn also honors a user's choice in restricting profile visibility from search engines. LinkedIn, *User Agreement*. Upon deletion of a user's account, the user's profile "may continue to be displayed in [search engine results] until they refresh their cache." LinkedIn, *Privacy Policy*.

In contrast, hiQ has no obligation to remove or permanently delete personal information upon request. hiQ aggregates data over time, including data the user deleted, and publishes that data to third parties for hiQ's commercial data. This

information may include hiQ's determination as to whether a LinkedIn user is a "flight risk" employee.

hiQ also provides a secretive risk score based on data obtained from LinkedIn. hiQ, *Enterprise Solutions* (2017).[20] hiQ sells this information to employers and other interested buyers. This data can result in sanctions, demotion, and termination. 4ER-593. This controversial practice is contrary to the interests of LinkedIn users and disfavored by experts in consumer protection. *See* Danielle Keats Citron & Frank A. Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 Wash. L. Rev. 1 (2014) (arguing for greater transparency and oversight of predictive algorithms, the use of which 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'"). "[T]hroughout 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* (2016).

[20] https://www.hiqlabs.com/new-index/.

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, EEOC (Oct. 13, 2016) (describing specifically hiQ Lab's data practices).[21]

LinkedIn represents to its users that it will provide "choices that allow [them] to opt-out or control how we use and share your data." LinkedIn, *Privacy Policy*. These choices are expressed both through the privacy settings and data control policies that the LinkedIn platform implements. For example, if a user chooses to maintain a public profile, then that profile can be indexed by search engines and found through certain specified mail and calendar services. LinkedIn, *Off-LinkedIn Visibility* (2017).[22] By forcing LinkedIn to make user data available to hiQ Labs, the lower court has essentially negated the bargain between LinkedIn and its users, and undermined the fiduciary relationship upon which the users agreed to transfer their personal data to LinkedIn.

[21] https://www.americanbar.org/content/dam/aba/events/labor_law/2017/03/err/papers/steele_paper.authcheckdam.pdf.
[22] https://www.linkedin.com/help/linkedin/answer/79854.

C. LinkedIn's user agreement and privacy policy establish a fiduciary relationship with users.

As the data collector, LinkedIn bears the burden of protecting a user's personal information and ensuring data is only collected, used, and disclosed consistent with the company's terms, settings, and LinkedIn's representations. The lower court order ignores this existing relationship between LinkedIn users and the company.

The personal data submitted by users to LinkedIn is subject to the terms outlined in the company's agreement. LinkedIn, User Agreement (2017).[23] The User Agreement and Privacy Policy impose several restrictions on what LinkedIn can do with users' personal data. The Agreement limits disclosure of profile data, links, postings, and other communications. *Id.* at § 2.5. LinkedIn represents that "[w]here we have made settings available, we will honor the choices you make about who can see content or information." *Id.*

LinkedIn's User Agreement establishes a commitment to its users that it will restrict practices by third parties intended to obtain user data. LinkedIn states that any entity using their platform can be subject to restriction, suspension, or termination if they are "in breach of this Contract or law or are misusing the Services." *Id*. at § 3.4. That includes the specific prohibition against anyone who

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

attempts to "[d]evelop, support or use software, deices, scripts, robots, or any other means or processes (including crawlers, browser plug-ins and add-ons, or any other technology or manual work) to scrape the Services or otherwise copy profiles and other data from the Services." *Id*. at § 8.2. That also includes any attempt to "[b]ypass or circumvent any access controls or Service use limits (such as caps on keyword searches)" or to "[c]opy, use, disclose or distribute any information obtained from the Services, whether directly or through third parties (such as search engines), without the consent of LinkedIn." *Id.* LinkedIn specifically monitors searches of its user profiles to detect and prevent any unauthorized "commercial use" of personal data. LinkedIn, *Commercial Search Limit* (2017).[24] LinkedIn has already restricted over 11 million accounts for engaging in behavior violating the User Agreement, including scraping. 3ER-432.

LinkedIn not only prohibits misuse of user data; the company also relies on technological measures to limit access to user data. LinkedIn maintains a variety of systems that monitor and detect suspicious activity and restrict undesirable activity if necessary. For instance, LinkedIn's FUSE system limits and prevents the use of automated technology to scrape data from a substantial volume of member profiles (public or private). 4ER-760. To differentiate user activity from non-human activity, LinkedIn uses their Quicksand system to protect user information from

[24] https://www.linkedin.com/help/linkedin/answer/52950.

third-party scrapers. 4ER-760. Once undesirable activity has been detected (i.e. scraping), LinkedIn's Sentinel system restricts and even blocks further activity from that particular IP address. 4ER-760. LinkedIn's Org Block system generates a list of known bad IP addresses serving as large-scale scrapers. 4ER-760. And its Member and Guest Request Scoring System also restricts automated, non-human access for scraping purposes. The System monitors page requests made by visitors not logged into LinkedIn. It detects unusual patters and if it finds an unusual frequency of page requests by a non-user, the System will prevent further page requests and access to profile information and direct the user to LinkedIn's login page. 4ER-760.

These systems are designed to detect and differentiate normal user behavior, such as viewing public profiles to network and make connections on an individual basis, from automated aggregating acts as a privacy protective measure that limits third-party access to users' profiles. For example, LinkedIn has configured its "robots.txt" files to prohibit unauthorized bots and crawlers from accessing user profiles. 4ER-761. LinkedIn blocks approximately 95 million attempts by automation to scrape data on a daily basis. 4ER-761. Users rightfully expect LinkedIn to implement these access restrictions. By prohibiting LinkedIn from implementing these measures, the lower court has effectively eliminated key techniques that protect the privacy of user data.

LinkedIn's technique for limiting access by third parties is widely followed by many Internet firms to prevent automated "scraping." For example, the Completely Automated Public Turing test to tell Computers and Humans Apart technique ("CAPTCHA") is a widely used "challenge-response test used in computing to determine whether or not the user is human." CyLab, Security and Privacy Institute, Carnegie Mellon University, *The reCAPTCHA Project* (2017).[25] Such techniques are intended to ensure that personal data provided by users online for a particular purpose is not seized by others and repurposed.

II. The lower court injunction, which is contrary to the purpose of modern privacy law, is also contrary to the public interest.

The lower court order is not only contrary to the interests of individual LinkedIn users, it is contrary to the public interest because it undermines the principles of modern privacy and data protection law. That is significant in this case. LinkedIn has "over 500 million members in over 200 countries worldwide," LinkedIn, *About Us* (2017). The lower court order would subject all of these individuals to the whims of any company, anywhere to make use of their personal data however they choose, which is entirely contrary to privacy law.

The central purpose of modern privacy law is to ensure the ability of individuals to control the collection and use of their personal data held by others.

[25] https://www.cylab.cmu.edu/partners/success-stories/recaptcha.html.

This approach was set out in the "Fair Information Practices" in the United States in the 1970s, and then adopted by the Organization for Economic Cooperation and Development ("OECD") in 1980 as a global standard. Marc Rotenberg, *Fair Information Practices and the Architecture of Privacy*, 2001 Stan. Tech. L. Rev. 1, ¶¶ 43, 44. The "OECD Guidelines reflect a broad consensus about how to safeguard the control and use of personal information in a world where data can flow freely across national borders. Just as it does today on the Internet." *Id.* at ¶ 47. These principles of "Collection Limitation; Data Quality; Purpose Specification; Use Limitation; Security Safeguards; Openness; Individual Participation; and Accountability" still govern international privacy standards today, and it is "generally understood that the challenge of privacy protection in the information age is the application and enforcement of Fair Information Practices and the OECD Guidelines." *Id*. at ¶ 45.

The OECD Guidelines provide that "personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept-up-to date." Org. Econ. Co-operation and Dev., *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (Sept. 23, 1980); *see also* Privacy Law Sourcebook 482,

485 (Marc Rotenberg ed. 2016) (OECD Privacy Guidelines).[26] In other words, the quantity and type of data collected should be proportional to the purposes for which the data is being used. Furthermore, "the purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purposes." OECD Privacy Guidelines, *supra.* In specifying the purpose for which data is to be used, users providing their personal data maintain an expectation that their data will not be used for a different purpose. It is within the public interest that the use of data stay limited to the original purpose for which the data was retrieved in the first place.

The OECD guidelines also provide that "personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with [the principle stated prior] except: a) with consent of the data subject; or b) by authority of law." *Id.*

Processing personal data consistent with user expectations is essential to complying with modern data protection law. A company cannot simply gather and repurpose data it has collected without first obtaining a user's consent or

[26] http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

authorization required by law. It is therefore in the public interest for companies collecting personal data to properly limit unauthorized and secondary uses of that data not consistent with the purpose and scope of the original disclosure. In order to do so, companies must be able to guarantee to their users that they will only grant access to personal data in ways consistent with the user's expectations. Furthermore, companies should restrict access and repurposing of user data by third-parties where the user has not explicitly authorized such access.

The lower court's injunction ignores a company's attempt to limit the collection and use of personal data it has obtained. This is at odds with the core purpose of modern privacy law. Prohibiting companies such as LinkedIn from implementing technological and legal safeguards for user data is not only against the individual users' interests, it could also subject LinkedIn to fines or suits in many jurisdictions around the world. Users likely would have chosen not to create an account with LinkedIn if they had known that their personal data would be acquired by others to build profiles that would be sold back to their employers.

The public interest weighs against an injunction that undermines the modern concept of privacy and the specific interests of LinkedIn users.

CONCLUSION

EPIC respectfully requests that this Court reverse the lower court's preliminary injunction and remand the case for further consideration in light of the privacy interests of LinkedIn users.

October 10, 2017

Respectfully submitted,

/s/ Marc Rotenberg

Marc Rotenberg
Alan Butler
Electronic Privacy Information Center
1718 Connecticut Ave. NW
Suite 200
Washington, DC 20009
(202) 483-1140

Counsel for Amicus Curiae

CERTIFICATE OF COMPLIANCE

This brief complies with the type-volume limitation of Fed. R. App. P. 29(a)(4) because it contains 4,061 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii). This brief also complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in a proportionally spaced typeface using Microsoft Office Word for Mac in 14 point Times New Roman style.

/s/ Marc Rotenberg

Dated: October 10, 2017 Marc Rotenberg

CERTIFICATE OF SERVICE

I hereby certify that on October 10, 2017, I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the Ninth Circuit by using the CM/ECF system. I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the CM/ECF system.

/s/ Marc Rotenberg

Dated: October 10, 2017 Marc Rotenberg