No. 19-15472

In the

United States Court of Appeals
For the Ninth Circuit

AMERICAN CIVIL LIBERTIES UNION FOUNDATION, AMERICAN CIVIL LIBERTIES UNION OF NORTHERN CALIFORNIA, ELECTRONIC FRONTIER FOUNDATION, AND RIANA PFEFFERKORN,

Movants–Appellants,

v.

UNITED STATES DEPARTMENT OF JUSTICE, *et al.*,
Respondents–Appellees.

On Appeal from the United States District Court for the Eastern District of California
Case No. 1:18-mc-00057-LJO-EPG

BRIEF OF UPTURN AND COMPUTER SECURITY EXPERTS AS *AMICI CURIAE* IN SUPPORT OF MOVANTS-APPELLANTS

Phillip R. Malone
CA Bar No. 163969
JUELSGAARD INTELLECTUAL PROPERTY AND INNOVATION CLINIC
Mills Legal Clinic at Stanford Law School
559 Nathan Abbott Way
Stanford, California 94305-8610
(650) 725-6369
jipic@law.stanford.edu

Counsel for Amici Curiae

CORPORATE DISCLOSURE STATEMENT

Pursuant to Federal Rule of Appellate Procedure 26.1, counsel discloses that *amicus* Upturn, is a nonprofit corporation organized under the laws of the District of Columbia, that it does not have any parent company, and that no publicly held corporation owns 10% or more of its stock.

Dated: June 19, 2019

s/ Phillip R. Malone

Phillip R. Malone
CA Bar No. 163969

JUELSGAARD INTELLECTUAL PROPERTY AND INNOVATION CLINIC
Mills Legal Clinic at Stanford Law School
559 Nathan Abbott Way
Stanford, California 94305-8610
(650) 725-6369
jipic@law.stanford.edu

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

INTEREST OF *AMICI CURIAE*[1]

Amici are a number of noted computer scientists and computer security experts and the organization Upturn.[2] Biographies of the individual *amici* are in the Appendix.

Amicus Upturn is a 501(c)(3) nonprofit organization based in Washington, D.C. that works in partnership with many of the nation's leading civil rights and public interest organizations to promote equity and justice in the design, governance, and use of digital technology. Upturn's research and advocacy combines technical fluency and creative policy thinking to confront patterns of inequity, especially those rooted in race and poverty. One of Upturn's key priorities is to ensure that technology in the criminal justice system, including law enforcement technologies, supports civil rights and functions fairly. Another key Upturn priority is to ensure that people in the United States and around the world can meaningfully communicate over a free, open, and secure internet. This includes working to develop and deploy

---

[1] This brief is submitted pursuant to Rule 29(a) of the Federal Rules of Appellate. Pursuant to Rules 29(a)(4)(E) of the Federal Rules of Appellate Procedure, no part of this brief was authored by either party's counsel, neither party or their counsel contributed money that was intended to fund preparing or submitting the brief, and no person—other than the *amici* and their counsel—contributed money that was intended to fund preparing or submitting the brief. All parties have consented to the filing of this brief.

[2] *Amici* wish to thank Stanford Law School Juelsgaard Intellectual Property and Innovation Certified Law Student Claire Santiago for her substantial assistance in drafting this brief.

anti-censorship software and policy support for issues related to privacy and digital security.

Amici submit this brief because they believe that transparency around and public access to court decisions regarding the scope of government surveillance powers are essential to ensure the ability of users everywhere to engage with confidence in secure online communications and other activities, and to protect innovation and help maintain security on the internet.

SUMMARY OF ARGUMENT

Individuals cannot know, or obey, laws they cannot read. When a court decides a case, it applies and explains the law—and that precedent is used by and against individuals in subsequent cases. It is also used to decide how to structure one's personal and business activities in ways that comply with that law and that rely on reasonable expectations of what that law is. Access to the law ensures that individuals and organizations can trust that they know the bounds of the government's power to conduct surveillance and investigations—even if they are not permitted to know the precise methods. At issue in this case is that very trust. Internet users, security professionals, and the public at large need to know whether the government can force companies and technologists to expend resources to change their code and allow the government access to otherwise encrypted materials.

The district court's decision denying appellants' motion to unseal, however, leaves security professionals, companies, and internet users in the dark. They are deprived of the judicial reasoning explaining what the law is—and can only speculate as to what their potential responsibility to the government may be in a similar case.

In the meantime, security experts and organizations, like *amici*, have to grapple with the unverifiable speculation which is the information about this sealed case. Lack of access to the district court's decision creates considerable uncertainty about the security of people's communications over the internet. This uncertainty is dangerous for all internet users, but the risks are especially acute for many vulnerable users, such as human rights activists and victims of domestic violence. Users, wary of potential backdoors being built for the government by companies, could decline to update their software with the latest security fixes. In doing so, their device becomes a vulnerability for the entire system—an unvaccinated host susceptible to contract, and spread, computer viruses and other types of malware.

Unsealing the materials requested by Movants in this case would shine daylight on the judicial reasoning involved, inform technologists and companies about whether and how developers may be required to alter their code for the government, and allow technologists to dispel the uncertainty that threatens to damage user trust. All this could be done without requiring the government to

disclose details of any ongoing investigation or particular investigative techniques that are the proper subject of a sealing order.

ARGUMENT

I. THERE IS A COMPELLING PUBLIC INTEREST IN ACCESS TO COURT RULINGS THAT DEFINE THE GOVERNMENT'S POWER TO REQUIRE COMPANIES TO COMPROMISE ENCRYPTION AND SECURITY.

This case arises from a dispute over whether the United States can compel private companies to alter their products to enable surveillance that would not otherwise be possible given the original careful and deliberate design of those products. But the current appeal does not call on this Court to resolve the underlying questions about the scope of the government's power. Rather, it asks this Court only to ensure that the public—including security technologists and researchers like *amici*, similarly situated companies, and internet users at large—can have access to the law and legal reasoning used by the district court to address those questions. Access and transparency are critically important in this case.

A. The Public's Interest in Understanding the Legal Bounds of Government Eavesdropping Is Especially High Given the Dramatic and Unprecedented Nature of the Wiretap Request.

There is a public interest of the highest order in ensuring that our communications, and the overall security and integrity of our communications systems such as the internet, are protected and not undermined by private actors or the government. This case is especially significant because it is the latest chapter in

an ongoing debate over tension between greater security and privacy and the government's interest in access to information. That debate garnered great attention during the 2016 controversy over the the FBI's attempts to compel Apple to create unique software that would override an iPhone's failsafe—a security measure that wipes the phone if someone tries to use a brute force attack to unlock it—and thereby access the contents of an iPhone as part of the San Bernardino terrorism investigation. *See* Alina Selyukh, *A Year After San Bernardino and Apple-FBI, Where Are We On Encryption?*, NPR, Dec. 3, 2016, https://www.npr.org/sections/alltechconsidered/2016/12/03/504130977/a-year-after-san-bernardino-and-apple-fbi-where-are-we-on-encryption. Apple's CEO Tim Cook released an open letter urging Apple's view that doing as the government wished would undermine security for all iPhone users. Tim Cook, A Message to Our Customers, Feb. 16, 2016, https://perma.cc/5JBK-5ZHT. Numerous Congressional hearings followed, with the entire debate reflecting the tremendous significance of these issues for both law enforcement and for the security of users' devices and information. See ACLU Foundation Opening Brief (hereinafter "ACLU Opening Br."), at 11-15 and n. 7-10. And the issues raised in that case remain significant and pressing.

In the present case, the United States apparently was not demanding that Facebook facilitate a typical wiretap. Instead, from what *amici* can glean from

limited news reports and from Movants-Appellants' opening briefs on appeal, the government insisted that Facebook create a new capability, one that did not currently exist, to decrypt and enable access to certain Facebook Messenger voice calls, which are end-to-end encrypted. See Dan Levine & Joseph Menn, *US Government Seeks Facebook Help to Wiretap Messenger*, Reuters, Aug. 17, 2018, https://perma.cc/MM9M-C2XU (hereinafter "Levine and Menn, Aug. 17, 2018"); ACLU Opening Br. at 9-11. Facebook reportedly protested when declining to comply with the government's request that "it could only comply with the government's request if it rewrites the code relied upon by all its users to remove encryption or else hacks the government's current target . . . ." Levine and Menn, Aug. 17, 2018. The government's demands thus constituted a virtually unprecedented requirement that the company create security "backdoors" for the government's use, backdoors that could reduce the security and safety of all users.

Breaking end-to-end encrypted communications is, by design, not something Facebook can do easily, if at all. End-to-end encryption plays such a key role in ensuring online security and confidentiality precisely because of its unique characteristics. When a call, or a message, is end-to-end encrypted, "the only people who can read the messages are the people communicating." Andy Greenberg, *Hacker Lexicon: What is End-to-End Encryption?*, Wired, Nov. 25, 2014,

https://perma.cc/4M2R-PCD3. This is significantly more secure and protective than other ready means of securing communications.

By way of analogy, a typical unencrypted communication is similar to mailing a postcard—one writes one's message and places it in the mail, but anyone handling the mail, or a thief (a "hacker") who opens the mailbox, is able to read everything that was written. If, on the other hand, the letter (communication) is end-to-end encrypted, that would be equivalent to placing the letter in an unbreakable, armored pouch that could only be unlocked with a unique code pre-arranged with the recipient, and then sending the pouch and letter in its securely locked state through the mail. The postman (or Facebook, in this case) cannot gain access to the contents of the letter in any way; only the intended recipient can. The only way for the postman (or Facebook) to get access to the letter would be reengineer the entire postal system and only accept a new type of armored pouch to which the postman has the master access code. Doing so, however, would fundamentally alter the security and confidentiality not only of the target's armored pouch and mail but of *everyone*'s pouch and mail. The settled expectations and critical reliance interests of our entire online communications ecosystem would be dramatically undermined by any such requirement.

Thus, the government's demand that Facebook wiretap end-to-end encrypted Messenger voice calls constitutes a novel and extremely significant expansion of

government surveillance power. It is unlike a traditional wiretap, which typically involve someone physically tapping phone lines, or more recently used "wiretaps," which may entail companies installing software on a device that allows the government to listen in on communications at their "endpoints" prior to the call being encrypted.

Because of both the novelty and the extraordinary implications for security generally of the government's wiretap request, there is an extremely powerful public interest—for the public at large, security technologists, and other companies—in understanding the government's ability to compel entities and individuals to comply with such requests and any legal basis for it. Facebook reportedly also asserted in the lower court proceedings that the statute that authorized the wiretap order does not provide authority to compel Facebook to rewrite its products and change security for all users. ACLU Opening Br. at 10.

Many news articles reporting on this case have described the importance of information in the sealed docket and order because "depending on what specific relief the government sought from the court, the case may signal a potentially significant threat to the security of internet-based communications." Greg Norjem, Eric Wenger & Marc Zwillinger, *FBI vs. Facebook: What's at Stake?*, Ars Technica, Oct. 2, 2018, https://arstechnica.com/tech-policy/2018/10/fbi-vs-facebook-messenger-whats-at-stake/. *See also* Levine and Menn, Aug. 17, 2018 ("The

potential impact of the ruling is unclear . . . law enforcement agencies forcing technology providers to rewrite software to capture and hand over data that is no longer encrypted would have major implications.").

While there may well be portions of the lower court's ruling that address specifics of the investigation or the precise communications at issue that should legitimately remain sealed, there can be no legitimate argument for keeping the legal reasoning secret. The decision at issue addresses (and apparently resolves) legal questions of great importance to the security community and users. Unsealing those portions of the order need not include any disclosure of specific evidence, investigative details, conversations at issue, etc., in this case, but must include public access to the court's legal reasoning and the basic contours of the government's request and Facebook's objections.

B. Lack of Access to the District Court's Decision Furthers Uncertainty and Confusion About Whether the Law May Require Companies to Compromise the Security of Their Products.

The broad public interest in knowing how government surveillance may impact internet and communications security is thwarted by the district court's overbroad and unjustified sealing of its docket and opinion in this case. So long as those materials remain sealed, no one, aside from Facebook and the Department of Justice, can know whether and why, or why not, the government can use 18 U.S.C. § 2518(4) (the "Wiretap Act") or the All Writs Act, 28 U.S.C. § 1651(a), to compel

internet companies to break encrypted communications or hack their targeted electronic devices Reports indicate that Facebook argued to the court below that engineering a way to provide the government with access to Messenger voice calls was beyond the scope of the Wiretap Act's "technical assistance' provision". See Ellen Nakashima, *Facebook Wins Court Battle Over Law Enforcement Access to Encrypted Phone Calls*, Wash. Post, Sept. 28, 2018. And to the public's knowledge, the government has never successfully applied the Wiretap Act to an internet-based social media company or communications platform.[3]

But unfortunately, here the public has no way of confirming on what grounds and what theories the government attempted to compel Facebook to comply with a wiretap. All the public knows is that the government attempted to force an

---

[3] Under a separate statute, the Communications Assistance for Law Enforcement Act, "providers who offer covered services in the [United States] must be capable of implementing a wiretap upon receipt of a lawful order from the courts—and cannot argue that their technology is incapable of doing so." Greg Norjem, Eric Wenger & Marc Zwillinger, *FBI vs. Facebook: What's at Stake?*, Ars Technica, Oct. 2, 2018, https://arstechnica.com/tech-policy/2018/10/fbi-vs-facebook-messenger-whats-at-stake; *see also* 47 U.S.C. 1002(a). Nonetheless, "information services providers" including "electronic messaging services" were specifically exempted from this requirement by Congress. 47 U.S.C. §1002(b)(2). The Act also prevents the government from requiring even a covered service provider to utilize or adopt any specific design of services or features, 47 U.S.C. §1002(b)(3), or to decrypt communications unless the carrier possesses the information necessary to decrypt. 47 U.S.C. §1002(b)(1)(A).

information services provider to create for the government a new mechanism to wiretap otherwise inaccessible, end-to-end encrypted voice calls.[4] Unsealing the lower court's order that apparently declined to hold Facebook in contempt, and allowing the public, technologists, policymakers, and other companies to know the legal basis for the court's conclusions about the metes and bounds of the government's power to compel decryption, is the only way to mitigate the confusion and uncertainty brought about by the decision.

The strong public interest in understanding how surveillance affects the integrity of important communications systems readily outweighs the asserted, but not specifically articulated or documented, interests in secrecy relied on by the district court to justify its refusal to unseal *any* of the underlying decision. *United States v. Bus. Of Custer Battlefield Museum*, 658 F.3d 1188, 1195 (9th Cir. 2011) (courts must articulate the "compelling reasons" for sealing that outweigh the public policies favoring disclosure and "conscientiously balance" any competing interests).

---

[4] The uncertainty and confusion caused by the sealed order in this case only adds to the uncertainty that remains from the 2015 Apple-FBI controversy. While that dispute played out for a time in court and in Congress, it eventually ended without a legal resolution or clarity about the relevant law when the FBI successfully found a third party capable of unlocking the phone for a fee. Beyond the knowledge that the government was demanding that companies build backdoors and weaken security to ensure investigative access, no light was shed on whether or not the government can legally compel a company to take such steps.

In this case, however, the district court did not adequately consider, if it considered at all, the significant weight that should be given to the public's rights of access to the materials at issue based on the intense public interest and importance of those materials. Nor did the court attempt to balance those interests against any interests that might weigh in favor of continued sealing.

C. Uncertainty and Confusion Caused by the Sealed Decision Threaten Critical Reliance on Encryption and Undermine Vital User Trust.

The uncertainty over the legal basis for and the nature and scope of any government power to force companies to undermine end-to-end encryption erodes the trust that users and other software developers need to have in that encryption. Loss of trust harms individual users, companies, the public, and the security and integrity of the internet as a whole.

1. Vast numbers of companies, organizations and users that need to trust and depend on critical protections of end-to-end encryption are harmed by uncertainty.

Protecting the security and safety of electronic communications and other online activity is one of the most important challenges facing our society and the companies and technologists that society trusts to ensure that security. "It is impossible to operate the commercial Internet or other widely deployed global communications network with even modest security without the use of encryption." Harold Abelson, *et al.*, *Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications*, MIT Computer Science and

Artificial Intelligence Laboratory Technical Report, MIT-CSAIL-TR-2015-026, July 6, 2015, at 7, https://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf?sequence=8 (hereinafter "Keys Under Doormats"). Although vast changes have swept across computing and networks since the 1990s, today "the fundamental technical importance of strong cryptography and the difficulties inherent in limiting its use to meet law enforcement purposes remain the same. What has changed is that the scale and scope of systems dependent on strong encryption are far greater, and our society is far more reliant on far-flung digital networks that are under daily attack." *Id*. at 7-9.

Strong security is critical across the vast range of activities, communications, and transactions that are now conducted extensively, sometimes almost exclusively, online. Some of the most apparent and significant applications include health care, medical information, banking and other financial transactions, critical infrastructure applications, and all manner of personal communications. *See generally*, Consumers Union, *Beyond Secrets: The Consumer Stake in the Encryption Debate*, Dec. 21, 2017, https://advocacy.consumerreports.org/wp-content/uploads/2017/12/Beyond-Secrets-12.21.17-FINAL.pdf/. Going forward, as so-called smart homes and the "internet of things" result in billions of everyday devices being connected to the internet, the need for reliable and robust security will be even more critical.

But beyond these obvious needs are a host of other online activities where users' and providers' expectations about the reliability and security of encryption also are critical. For examples, human rights organizations, civil rights advocates, and other vulnerable users around the world rely, sometimes at risk to their lives, on knowing that the use of certain encrypted technologies will keep their communications secure. *See, e.g.*, National Academies of Sciences, Engineering, and Medicine, *Decrypting the Encryption Debate: A Framework for Decision Makers*. Washington, DC: The National Academies Press (2018), at 34, https://www.nap.edu/read/25010/chapter/5. ("In practice, encryption has come to play a more and more critical role in the work of journalists, human rights advocates, lawyers, public activists, and private communities of faith and opinion.").

Domestic violence survivors and support organizations, and government agencies that serve them, also must trust and rely on reliable encryption to protect their communications and activities from interception. *See* Technology Safety, *Smartphone Encryption: Protecting Victim Privacy While Holding Offenders Accountable*, April 12, 2016, https://www.techsafety.org/blog/2016/4/12/smartphone-encryption-protecting-victim-privacy-while-holding-offenders-accountable/. Journalists, too, require confidence in the security of the tools they use to gather information and communicate with and protect valuable confidential sources. *See, e.g.*, Brief of *Amici*

Curiae The Reporters Committee for Freedom of the Press and 23 Media Organizations, at 24-30, *ACLU, et al., v. US DOJ, et al*., Nos. 19-1547219-15473. These are just a few of many similar examples.

Security professionals and researchers play vital roles in creating and maintaining secure online systems, and in helping individuals, businesses, and organizations implement and understand the reliability of the encryption technologies on which those individuals and groups depend. Professionals themselves must trust and have confidence in their knowledge of how end-to-end encryption operates and any limits on the protection it provides. They need to be able to trust the tools they use, and to accurately communicate to users, companies, and the world at large what security technologies can and cannot do.

Trust is a fundamental element of building secure and widely used software and tools.[5] Thus, for security professionals and researchers, knowing the permissible scope of government surveillance capabilities and the legal basis for any government

---

[5] For example, Signal is considered by many to be an extremely secure messaging app in part because it is open source, meaning that anyone can examine its code to verify that it is as secure as its makers claim and to probe for vulnerabilities. *See* Michael Grothaus, If You value Your Privacy, Switch to Signal As Your Messaging App Now, Fast Company, April 19, 2019, https://www.fastcompany.com/90335034/if-you-value-your-privacy-switch-to-signal-as-your-messaging-app-now.

actions that might (or might not) require companies to undermine end-to-end encryption, and under what circumstances, is critical to the important work these professionals and researchers do.

For all of these uses, trust in the security provided by encryption is essential. When that trust is eroded, as it is by the uncertainty over whether and when the government may use the law to require trusted providers to break the encryption these individuals and groups rely on, important communications may be limited and valuable activities and transactions impeded. The kind of uncertainty and confusion that is created by sealing the docket and court decision in a significant case like the current one is particularly damaging to this essential trust.

2. The security of the internet and its ecosystems is harmed by the erosion of trust caused by uncertainty and confusion over government wiretap powers.

Beyond these examples of specific applications where trust in encryption is essential, the security and integrity of the internet overall and its resistance to hacking, malware, surveillance, and cyberattacks also depend on user trust. One of the key components to keeping the internet, as well as emerging networks of internet-of-things devices, protected from these types of threats is keeping software up-to-date and secure. And by far the best currently available tool for doing that is automatic updates from software and platform vendors, including Facebook, Microsoft, and thousands more. These updates "automatically" update the

underlying program, often applying critical "patches" that serve to eliminate newly discovered security flaws or vulnerabilities.

As one of the *amicus* computer security experts on this brief has previously explained,

> security in the modern internet can be understood as something of an ecosystem, where survival depends on continually adapting to protect against ever-evolving new threats. Vendor software updates, applied at regular intervals, are, for better or worse, the only large-scale method we have for adapting our defenses. Those who fail to update become prominently attractive targets, with their computers succumbing to automated attacks that might do anything from steal personal information to installing "ransomware" that holds important files hostage until payment is made.

Matt Blaze, *Stop Ignoring Those "Update Your Device" Messages*, New York Times, March 27, 2019, https://www.nytimes.com/2019/03/27/opinion/asus-malware-hack.html/. "Programmers and criminals are in a perpetual information-security arms race. Widely deployed software must be regularly updated or it will quickly become insecure. And consumers depend on manufacturers to deliver frequent software updates to 'patch' vulnerabilities as they are identified." Beyond Secrets at 16-17.

Auto-updates are so effective in part because they are, by definition, automatic (unless users disable them) and therefore extremely convenient, requiring little or no effort and no technical savvy from users. In the case of some auto-updates, such as those on the iPhone, the user must affirmatively accept the update, but still little

effort or knowledge is needed. Users are more likely to end up with security updates installed when there is little or nothing they need to do to make the installation happen, other than choosing to enable (or not to disable) auto-updates. *Id*. at 17 (automatic updates are "so appealing [because the] user does not have to do anything to benefit from security and performance improvements.").

It is difficult to overstate the importance of automatic updates in helping to maintain the security of the internet and the individual devices connected to it, including smartphones. According to another computer security expert, "many security experts think of the automatic update mechanisms as . . . a public health system for the Internet." Does the FBI Need a Back Door to Your Data?, KCRW (Feb. 23, 2016), http://www.kcrw.com/news-culture/shows/to-the-point/apple-v-fbis-iphone/unlock-battle#seg-does-the-fbi-need-a-back-door-to-your-data . (comments of Christopher Soghoian; "We are all better off when consumers automatically receive software updates.").

For automatic updates to work and to play this vital role in protecting the internet, however, individual users *must trust their software vendor and trust the update*s. Consumers need to have confidence that software updates will enhance their security, not undermine it. "[P]eople need to know that they can trust software updates." Jack Gillum and Aaron C. Davis, *Local Governments Keep Using This Software, But it Might Be A Backdoor for Russia*, The Washington Post, Jul. 23,

2017, https://www.washingtonpost.com/investigations/local-governments-keep-using-this-software--but-it-might-be-a-back-door-for-russia/2017/07/23/39692918-6c99-11e7-8961-ec5f3e1e2a5c_story.html?utm_term=.a36b56aaa0b4 (quoting Joseph Lorenzo Hall, chief technologist at the Center for Democracy and Technology). Greg Norcie, *Yes, You Should Always Update Your Software*, CDT Blog, May 3, 2016, https://cdt.org/blog/yes-you-should-always-update-your-software/.

But uncertainty over whether and how software companies like Facebook may be forced by the government to create and distribute new "vulnerabilities" that break encryption and make users' communications insecure can destroy this critical trust in a very direct and powerful way. If Facebook, or Apple, or another software or communications provider can be compelled to design and deploy a new "broken" version of encryption or purposefully insert a new insecurity, the most likely way that insecurity will be delivered is through an automatic update. The uncertainty over when and how the law may require companies to compromise users security, exacerbated by the lack of access to the lower court's reasoning and conclusions in this case, undermines user trust and may well lead users to disable automatic updates or, in the case of the devices like the iPhone, to refuse to accept them when they are delivered.

This loss of trust in auto-updates, whether from fear that they may implement a newly developed government capability to break encryption and monitor the user's communications, or from the occasional third-party hack of those updates, creates a significant danger "that people might be frightened away from installing the critical software updates that keep life on the modern internet relatively safe. . . . But disallowing updates brings a near certainty over time that we will be successfully attacked." *Id*. And the more individual devices that become vulnerable to attack because their users are afraid to automatically update them, the more devices there are to serve as attack vectors that can endanger the "public health" of the rest of the network. Confusion and uncertainty create greater risk for the entire network and jeopardize security for everyone.

II. THE SUPREME COURT AND THIS COURT HAVE RECOGNIZED THE CRITICAL RIGHT OF ACCESS TO JUDICIAL DECISIONS.

The Supreme Court has observed that "justice cannot survive behind walls of silence." *Sheppard v. Maxwell*, 384 U.S. 333, 349 (1966). Sunlight, and public accessibility, are critical to democracy and justice. In *Valley Broad Co. v. United States Dist. Court*, this Court echoed that sentiment, stating that public access to judicial reasoning and documents "helps the public keep a watchful eye on public institutions and the activities of government." 798 F.2d 1289, 1293 (9th Cir. 1986). More recently, this Court again upheld the principle that "the presumption of access

is 'based on the need for federal courts, although independent—indeed, particularly because they are independent—to have a measure of accountability and for the public to have confidence in the administration of justice.'" *Ctr. for Auto Safety v. Chrysler Grp., LLC*, 809 F.3d 1092, 1096 (9th Cir. 2016) (quoting *United States v. Amodeo* (*Amodeo II*), 71 F.3d 1044, 1048 (2d Cir.1995)).

In this case, as explained by Movants in the lower court and in their opening briefs on appeal, the public was left without a way to hold the courts accountable—and to have any information or certainty about the scope of government surveillance activities that profoundly affect their daily lives and daily choices about what software and communications tools to use, how to use them, whether to trust vital mechanisms like automatic updates, and more. Access to the lower court decision this case could assuage the fears of many, and affirm the "general right to inspect and copy public records and documents, including judicial records and documents." *Nixon v. Warner Commc'ns, Inc.*, 435 U.S. 589, 597 (1978).

CONCLUSION

For the foregoing reasons, the Court should reverse the decision below and order that the docket, appropriate portions of the district court's order, and any other appropriate materials be unsealed.

Dated: June 19, 2019

Respectfully submitted,

s/ Phillip R. Malone

Phillip R. Malone, CA Bar No. 163969

JUELSGAARD INTELLECTUAL PROPERTY AND INNOVATION CLINIC
Mills Legal Clinic at Stanford Law School
559 Nathan Abbott Way
Stanford, California 94305-8610
(650) 725-6369
jipic@law.stanford.edu

Counsel for Amici Curiae

CERTIFICATE OF COMPLIANCE

1. This **Brief of Upturn and Computer Security Experts as *Amici Curiae* in Support of Movants-Appellants** complies with the type volume limitation contained in Fed. R. App. P. 29(a)(5) and Ninth Circuit Rule 32-1(a), because it contains 4774 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(f).

2. This brief 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 Word in 14 point Times New Roman font.

By: s/ Phillip R. Malone
Phillip R. Malone
CA Bar No. 163969

Counsel for Amici Curiae

Dated: June 19, 2019

APPENDIX

LIST OF COMPUTER SECURITY EXPERT *AMICI*[1]

Harold Abelson. Dr. Harold "Hal" Abelson is a Professor of Electrical Engineering and Computer Science at MIT, a fellow of the IEEE, and a founding director of both Creative Commons and Public Knowledge. He directed the first implementation of the Logo computing language for the Apple II, which made the language widely available on personal computers beginning in 1981, and published a popular book on Logo in 1982. Abelson co-developed MIT's introductory computer science subject, which included innovative advances in curricula designed for students pursuing different kinds of computing expertise. These curricula had a worldwide impact on university computer science education. Notable awards include the Bose Award (MIT School of Engineering, 1992), the Taylor L. Booth Education Award (IEEE-CS, 1995), and the SIGCSE 2012 Outstanding Contribution to Computer Science Education (ACM, 2012). Abelson holds an A.B. from Princeton University and a Ph.D. in mathematics from MIT.

Steven M. Bellovin. Steven Bellovin is the Percy K. and Vida L.W. Hudson Professor of Computer Science and affiliate law faculty at Columbia University.

---

[1] Affiliation is provided for identification purposes only. All signatories are participating in their individual capacity, not on behalf of their institutions.

Matt Blaze. Matt Blaze is a professor at Georgetown University in the Department of Computer Science and at the Georgetown Law Center. His research focuses on cryptography, computer security, surveillance, election security, and the interaction of technology and public policy. Prior to joining Georgetown, he was a professor of Computer and Information Science at the University of Pennsylvania. He holds a PhD in computer science from Princeton University.

Whitfield Diffie. Dr. Whitfield Diffie serves as advisor to a variety of startups, primarily in the field of security. He is best known for discovering the concept of public key cryptography, which underlies the security of internet commerce and all modern secure communication systems. Dr. Diffie's two principal positions after leaving Stanford University in the late 1970s were Manager of Secure Systems Research for Bell-Northern Research, the laboratory of the Canadian telephone system, and Chief Security Officer at Sun Microsystems. Dr. Diffie received the 2015 Turing Award and in 2017 was elected to both the National Academy of Engineering and the Royal Society.

CERTIFICATE OF SERVICE

I hereby certify that I electronically filed the foregoing **Brief of Upturn and Computer Security Experts as *Amici Curiae* in Support of Movants-Appellants** with the Clerk of the Court of the United States Court of Appeals for the Ninth Circuit by using the appellate CM/ECF system on June 19, 2019.

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.

By: s/ Phillip R. Malone
Phillip R. Malone,
CA Bar No. 163969

Counsel for Amici Curiae

Dated: June 19, 2019