CASE NO. 19-16066

IN THE

United States Court of Appeals

FOR THE NINTH CIRCUIT

CAROLYN JEWEL, ET AL.,
Plaintiffs-Appellants,

v.

NATIONAL SECURITY AGENCY, ET AL.,
Defendants-Appellees.

ON APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA
CASE NO. 08-CV-04373-JSW
THE HONORABLE JEFFREY S. WHITE, UNITED STATES DISTRICT JUDGE

BRIEF FOR AMICUS CURIAE HUMAN RIGHTS WATCH IN SUPPORT OF PLAINTIFFS-APPELLANTS

WILSON SONSINI GOODRICH & ROSATI
Professional Corporation

LAUREN GALLO WHITE
KEVIN LAXALT-NOMURA
One Market Plaza
Spear Tower, Suite 3300
San Francisco, CA 94105
Telephone: (415) 947-2000
Facsimile: (415) 947-2099
lwhite@wsgr.com
knomura@wsgr.com

BRIAN M. WILLEN
BRIAN J. LEVY
1301 Avenue of the Americas
40th Floor
New York, NY 10019
Telephone: (212) 999-5800
Facsimile: (212) 999-5899
bwillen@wsgr.com
blevy@wsgr.com
Counsel for Amicus Curiae

CORPORATE DISCLOSURE STATEMENT

Pursuant to Fed. R. App. P. 26.1, the undersigned counsel for amicus curiae certifies that Human Rights Watch has no parent corporation and that no publicly held corporation holds 10% or more of its stock.

Dated: September 13, 2019

By: *s/ Brian M. Willen*
Brian M. Willen

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

CASES

RULES

LITIGATION DOCUMENTS

OTHER AUTHORITY

SECONDARY SOURCES

STATEMENT OF IDENTITY, INTEREST, AND SOURCE OF ITS AUTHORITY TO FILE

Human Rights Watch ("HRW") is a non-profit research and advocacy organization registered and headquartered in New York whose mission is to expose violations of international human rights, end abuses, and provide victims a voice. It does this by researching human rights conditions around the world and enlisting support from the public and international community for change. One focus of its work in the United States is challenges posed to online freedom of expression and the right to privacy by practices such as mass surveillance. HRW is also a plaintiff in *First Unitarian Church of Los Angeles v. National Security Agency*, No. 4:13-cv-03287-JSW (N.D. Cal.), a lawsuit that also objects to the Government's collection and retention of telephone communications records in conjunction with AT&T.

All parties have consented to the filing of this brief.

No party's counsel authored the brief in whole or in part or contributed money that was intended to fund preparing or submitting the brief. No person other than amicus curiae, its members, and its counsel contributed money that was intended to fund preparing or submitting the brief.

INTRODUCTION

The unlawful, far-reaching surveillance challenged in this case deprives everyday Americans of their basic human right to privacy. Moreover, such mass surveillance prevents HRW and all who seek to defend basic rights from fulfilling their core missions: discovering human rights abuses and working to expose and change them. Nevertheless, after more than a decade of litigation, the district court held that Plaintiffs lack standing under the state secrets privilege. HRW submits this amicus brief in support of Plaintiffs-Appellants to highlight two especially dangerous consequences of that mistaken ruling.

First, in this brief, HRW describes the ways in which illegal mass surveillance harms HRW's own operations and those of other human rights defenders, be they individuals or groups.[1] Human rights defenders, because of the nature of their work in exposing official abuses, are targets for surveillance by the United States and other governments. Where abuses of surveillance powers come to light around the globe, human rights defenders are often found to be the first victims. Under the district court's ruling, the Government will be able to continue to surveil telephone and Internet traffic, including that of HRW and the sources and activists it works to

[1] As used in this brief, "human rights defender" has the broad sense derived from United Nations General Assembly Resolution A/RES/53/144.

protect. Based on the Government's past willingness to surveil HRW and other human rights defenders, it is likely the Government will sift through the data collected from mass surveillance to target human rights defenders. This mass surveillance obstructs HRW's work, limiting its ability to investigate and expose human rights abuses. By throwing out Plaintiffs' effort to challenge the Government's unlawful surveillance, the district court's unduly narrow approach to standing—and its unduly broad approach to the state secrets privilege—allows this obstruction to continue.

Second, the district court's application of the state secrets privilege is tantamount to a holding that individuals can only sue to stop illegal surveillance when the Government admits to surveilling those individuals. This all but eliminates the possibility that anyone would have standing. This interpretation is both wrong on the law and invites the Government to conceal its activities, including through a deceptive practice known as "parallel construction." Through this practice, the Government reconstructs evidence obtained using electronic surveillance, such as by having an intelligence agency tip off separate law enforcement officers to seek that evidence, without explaining the basis of the tip. The Government then claims that the evidence was found independently from the surveillance, and thus that it need not disclose to defendants that they were surveilled ***even when that surveillance forms the basis of the Government's prosecution***. Such practices enable the Government to circumvent

its legal obligations—such as those required under Rule 16(a)(1)(E) of the Federal Rules of Criminal Procedure and *Brady v. Maryland*, 373 U.S. 83, 87 (1963)—to turn over evidence to a criminal defendant or disclose that it surveilled the defendant. The Court should consider the application of the state secrets doctrine taking into account its impact on basic principles of criminal justice as well as its potential to deprive anyone of standing to challenge serious constitutional harms.

ARGUMENT

I. UNREASONABLE LIMITATIONS ON STANDING CHILL HUMAN RIGHTS DEFENDERS

As Plaintiffs' opening brief explains (*see, e.g.*, Opening Br. 1–2, 67–68, 70), the Government's illegal collection of data directly harms millions of Americans. *See also* Bruce Schneier, Opinion, *NSA Robots Are 'Collecting' Your Data, Too, and They're Getting Away with It*, Guardian (Feb. 27, 2014) (explaining the danger of data collection);[2] G.A. Res. 68/167, at 1 (Dec. 18, 2013) (explaining that "surveillance, interception and data collection . . . may violate or abuse human rights").[3] And, as Plaintiffs' brief further explains, the district court's dismissal will allow that harm to persist indefinitely without even the possibility of legal recourse. *See* Opening Br. 1

[2] Available at: https://www.theguardian.com/commentisfree/2014/feb/27/nsa-robots-algorithm-surveillance-bruce-schneier.

[3] Available at: https://undocs.org/A/RES/68/167.

("The district court's dismissal . . . mak[es] it impossible to bring any litigation challenging the legality of such surveillance without the Executive's permission.").

But the consequences of the district court's ruling do not end there. The Government's unlawful mass surveillance also burdens human rights defenders, making it harder for them to fulfill their missions as shown in a 2014 joint report by HRW and the ACLU about how government surveillance burdens journalists and lawyers investigating government abuses. *See With Liberty to Monitor All: How Large-Scale US Surveillance Is Harming Journalism, Law, and American Democracy*, Human Rights Watch & ACLU (July 2014).[4] Among other things, surveillance causes sources to avoid talking to journalists, requires journalists to waste time and money to take prophylactic measures to avoid surveillance, and inhibits coverage of sensitive topics of public import. *See id.* at 22–48. Amnesty International similarly recognized that "[m]ass surveillance and targeted surveillance of [human rights defenders] – on and offline – continues to grow worldwide. . . . While mass surveillance is carried out by countries like the UK and the USA, the targeted surveillance of HRDs and others is

[4] Available at: https://www.aclu.org/sites/default/files/assets/dem14-withlibertytomonitorall-07282014.pdf.

commonplace in countries all over the world." *Human Rights Defenders Under Threat—A Shrinking Space for Civil Society* 19, Amnesty International (May 2017).[5]

When human rights defenders are required to try to stay ahead of the Government's sophisticated means of surveillance, they must redirect finite, limited resources away from their mission. When their work lags, it harms not only individuals, but national security. As the United Nations Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism reported in September 2015, human rights groups prevent the injustices that may lead disaffected individuals to join terrorist organizations:

> National and international non-governmental organizations (NGOs) can be key actors in effective counter-terrorism strategies. . . . They give a voice to disaffected or marginalized sectors of society, promote the needs of those who are politically, economically or socially excluded and deliver humanitarian relief in areas affected by conflict. . . .
>
> . . . .
>
> Mass surveillance powers, often justified on counter-terrorism grounds, have been used to target civil society groups, human rights defenders and journalists in a number of States.

[5] Available at: https://www.amnesty.nl/content/uploads/2017/05/HRD-briefing-26-April-2017-FINAL.pdf?x18276.

U.N. Special Rapporteur, *Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism* ¶¶ 7, 16, U.N. Doc A/70/371 (Sept. 18, 2015).[6]

In short, mass surveillance allows abuses to fester and jeopardizes Americans and others around the world.

A. HRW (And Other Human Rights Defenders) Have Been And Will Be Targeted By U.S. Surveillance

Human Rights Watch is composed of roughly 450 employees who work in the United States and around the world, investigating human rights abuses, reporting on their findings, and working with governments and civil society to change policies and address abuses. To perform this work, HRW communicates with sources in the United States and abroad. HRW's effectiveness and credibility depend heavily on being able to interview these sources because they have direct knowledge of human rights abuses. HRW's sources include government officials, individuals targeted for abuse, witnesses, dissidents, experts, and whistleblowers—all of whom may face substantial risk of harm for cooperating with HRW. Because HRW works with people who are knowledgeable about abusive practices, the organization faces heightened risks from the prospect of surveillance that make its work much more difficult.

[6] Available at: https://undocs.org/A/70/371.

Although HRW is the focus of this brief, numerous human rights organizations have been surveilled. This is especially true in countries governed by authoritarian regimes: "Governments across the world are increasingly attacking non-governmental organizations (NGOs) by creating laws that subject them and their staff to surveillance . . . ." *Global Assault on NGOs Reaches Crisis Point as New Laws Curb Vital Human Rights Work*, Amnesty International (Feb. 21, 2019).[7] For instance, Amnesty International found that, in 2019, "government-backed bodies" made "multiple attempts to gain access to the email accounts of several prominent Egyptian human rights defenders, media and civil society organizations' staff." *Phishing Attacks Using Third-Party Applications Against Egyptian Civil Society Organizations*, Amnesty International (Mar. 6, 2019).[8]

Surveillance is not limited to such countries. For instance, the United Kingdom Government Communication Headquarters illegally surveilled the Egyptian Initiative for Personal Rights and the South African NGO Legal Resources Centre. *See* Owen Bowcott, *GCHQ's Surveillance of Two Human Rights Groups Ruled Illegal by*

[7] Available at: https://www.amnesty.org/en/latest/news/2019/02/global-assault-on-ngos-reaches-crisis-point/.

[8] Available at: https://www.amnesty.org/en/latest/research/2019/03/phishing-attacks-using-third-party-applications-against-egyptian-civil-society-organizations/.

Tribunal, Guardian (June 22, 2015).[9] In Mexico, human rights defenders were targeted with "government-exclusive" spyware. John Scott-Railton et al., *Reckless Exploit Mexican Journalists, Lawyers, and a Child Targeted with NSO Spyware*, Citizen Lab (June 19, 2017).[10] And, as HRW and the ACLU reported, journalists covering national security explained that American surveillance is like "what one might find in more authoritarian countries." *With Liberty to Monitor All*, *supra*, at 47. Some have said that United States surveillance is even worse because of the Government's immense technical capabilities. HRW employees stressed the difficulty in trying to provide appropriate protections to their staff and sources from secret mass surveillance.[11]

The comprehensive collection of metadata at issue here is especially damaging to HRW. As one HRW researcher explained, the Government can use the metadata to surveil HRW researchers *retroactively*. That is, an HRW researcher might be able to avoid government surveillance when talking to sources prior to the publication of a report. But once the report has been published, the Government can search the

[9] Available at: https://www.theguardian.com/uk-news/2015/jun/22/gchq-surveillance-two-human-rights-groups-illegal-tribunal.

[10] Available at: https://citizenlab.ca/2017/06/reckless-exploit-mexico-nso/.

[11] Unless otherwise noted, the descriptions in this brief of the first-hand accounts of HRW employees were collected by counsel for amicus curiae in a series of interviews.

metadata of HRW—and any credited individuals—to learn about that researcher's communications during the investigation period.

1. The U.S. Government Has Surveilled And Will Continue To Surveil HRW

The Government likely has collected data from HRW through the AT&T program at issue in this case. HRW used AT&T as its cellular provider for all staff between September 2015 and July 2017 and still has a contract with AT&T for a very limited number of staff members. AT&T also provides HRW with WiFi connectivity in San Francisco.

HRW is especially concerned about the Government's ability to retroactively surveil it because of the evidence that the U.S. Government has previously targeted it for surveillance. For instance, when the Council of Europe asked if the NSA was surveilling "the 'highly sensitive and confidential communications'" of Amnesty International and HRW, whistleblower Edward Snowden responded, "The answer is, without question, yes. Absolutely." Luke Harding, *Edward Snowden: US Government Spied on Human Rights Workers*, Guardian (Apr. 8, 2014);[12] *see also* Compl., *First Unitarian Church of L.A. v. NSA*, No. 4:13-cv-03287-JSW (N.D. Cal. July 16, 2013), ECF No. 1 (alleging that HRW was a victim of the "Associational Tracking Program,"

[12] Available at: https://www.theguardian.com/world/2014/apr/08/edwards-snowden-us-government-spied-human rights-workers.

in which the National Security Agency indiscriminately obtained information from HRW and numerous other associations).

HRW's work makes it a natural target for surveillance. For instance, the HRW report, *The Dark Side*, deals with parallel construction. When asked for comment, the Government was reluctant to discuss its secretive tactics, with numerous agencies declining comment. *Dark Side: Secret Origins of Evidence in US Criminal Cases*, Human Rights Watch (Jan. 9, 2018).[13] Nonetheless, Human Rights Watch interviewed current and former U.S. government officials, including, among others, a "former federal prosecutor who requested anonymity." *Id.* Investigating and reporting on surveillance with such anonymous official informants makes HRW an especially vulnerable target of surveillance.

Similarly, in 2012, HRW issued a report, *Delivered into Enemy Hands: US-Led Abuse and Rendition of Opponents to Gaddafi's Libya*.[14] As the report's title suggests, HRW investigated the United States' unlawful rendition practices under which individuals were sent to Libya and tortured. The report originated from HRW's discovery of secret American documents discovered in Libya after the fall of the

[13] Available at: https://www.hrw.org/report/2018/01/09/dark-side/secret-origins-evidence-us-criminal-cases.

[14] Available at: https://www.hrw.org/report/2012/09/05/delivered-enemy-hands/us-led-abuse-and-rendition-opponents-gaddafis-libya.

Gaddafi regime. *See US/UK: Documents Reveal Libya Rendition Details*, Human Rights Watch (Sept. 8, 2011).[15] HRW recognized that its use of these documents subjected it to an extreme risk of surveillance. These are just two examples of the type of investigative work performed by HRW to expose abuse and unlawful conduct by the Government.

The Government also surveils journalists who, like HRW, report on intelligence and terrorism issues. Shortly after HRW's Libya report was published, the *New York Times* reported that the Obama administration "secretly seized two months of phone records for reporters and editors of The Associated Press" to learn about an Associated Press investigation into the CIA. Charlie Savage & Leslie Kaufman, *Phone Records of Journalists Seized by U.S.*, N.Y. Times, May 13, 2013, at A1. That same month, the public learned that the Obama administration seized a reporter's personal emails to investigate the reporter's alleged receipt of classified information. *See* Ann E. Marimow, *Records Offer Rare Glimpse at Leak Probe*, Wash. Post, May 20, 2013, at A01. HRW's work investigating government abuses, including with regard to terrorism and surveillance, makes it an obvious target for similar invasions.

[15] Available at: https://www.hrw.org/news/2011/09/08/us/uk-documents-reveal-libya-rendition-details.

The Government's previous willingness to surveil HRW, other human rights defenders, and journalists strongly suggests that the Government will sift through the data it collects through mass surveillance to target human rights defenders.

2. The Transnational Character Of HRW's Work Makes It A Target For U.S. And Foreign Surveillance

HRW's international work also increases its risk of being surveilled through mass surveillance because the U.S. Government has jurisdiction over American infrastructure through which foreign data can be routed. Moreover, the Government has shown increased willingness to conduct transnational surveillance. It claims heightened powers to surveil at the border and outside the country, and it shares intelligence with foreign governments.

Even entirely foreign communications are subject to American mass surveillance because the United States has jurisdiction over overseas communications made using the services or infrastructure of United States–based companies, such as AT&T. Much of the world's communications flow through that infrastructure even when users are not based in the United States. HRW's interim deputy director of its U.S. program explained that "[e]ven a transfer of data between parties in the same country may result in the data transiting via other countries without the sender or

recipient ever knowing." Laura Pitter, *Why U.S. Should Care About Surveillance Abroad*, CNN (Apr. 16, 2014).[16]

The Government's behavior shows its interest in transnational surveillance. With regard to borders, the Government contends that it is allowed to conduct virtually unfettered searches of any electronic device entering or exiting the country, including the entire contents of a user's computer. And the Government conducts these border searches with increasing frequency, with fiscal year 2017 searches estimated to quadruple 2015 searches. *See* Kaveh Waddell, *The Steady Rise of Digital Border Searches*, Atlantic (Apr. 12, 2017).[17] For instance, the Government reportedly turned away 17-year-old Palestinian Ismail Ajjawai, who was traveling to attend Harvard University, after searching Mr. Ajjawi's computer and social media accounts. *See, e.g.*, Graham Kates, *Harvard Freshman's Visa Rejected by Border Officers at U.S. Airport*, CBS News (Aug. 28, 2019).[18]

The Government's intrusive border searches recently resulted in a Ninth Circuit decision placing limits on the Government's policy. *See United States v. Cano*, ---

[16] Available at: https://www.hrw.org/news/2014/04/16/why-us-should-care-about-surveillance-abroad.

[17] Available at: https://www.theatlantic.com/technology/archive/2017/04/the-steady-rise-of-digital-border-searches/522723/.

[18] Available at: https://www.cbsnews.com/news/harvard-freshman-palestinian-student-rejected-by-cbp-border-protection-officer-at-boston-logan-airport/.

F.3d. ----, 2019 WL 3850607 (9th Cir. Aug. 16, 2019). In that case, this Court explained that forensic cell phone searches "require reasonable suspicion" and all "cell phone searches at the border . . . must be limited in scope to a search for digital contraband." *Id.* at *2. But in stark contrast to this holding, the Government contends it has virtually unlimited power to search devices. *See* Mem. Supp. SJ, *Alasaad v. McAleenan*, No. 1:17-cv-11730-DJC (D. Mass. June 6, 2019), ECF No. 97.

HRW employees frequently cross the border where they are exposed to abusive surveillance. Some do primarily transnational work, like those who research abuses at the United States–Mexico Border. Amnesty International reported that the U.S. Government is using warrantless surveillance to attack groups that aid migrants: "US authorities have subjected human rights defenders to warrantless surveillance, interrogations, invasive searches, travel restrictions, and, in isolated cases, a false arrest and unlawful detention." *'Saving Lives Is Not a Crime': Politically Motivated Legal Harassment of Migrant Human Rights Defenders by the USA*, Amnesty International (July 2, 2019).[19] Other HRW employees confront border issues because they are stationed full-time in foreign countries but regularly visit the United States.

[19] Available at: https://www.amnestyusa.org/reports/saving-lives-is-not-a-crime-politically-motivated-legal-harassment-of-migrant-human-rights-defenders-by-the-usa/.

Because of these intrusive searches, HRW worries that the Government might search HRW employees' devices. Some employees report security briefings before trips to Mexico that are half about the danger from gang and cartel violence and half about U.S. government surveillance.

In addition, the United States and foreign countries share intelligence, including the "'Five Eyes' arrangement with the United Kingdom, Australia, Canada, and New Zealand" and "unilateral agreements with countries like Germany, Israel, and Saudi Arabia." Brett Max Kaufman, *The U.S. Intelligence Community Can Share Your Personal Information with Other Governments, and We're Demanding Answers*, ACLU (June 13, 2017).[20]

Foreign governments have tried to surveil HRW. For instance, the German Federal Intelligence Service, known as "BND," "spied on NGOs," including HRW. Justin Huggler, *German Intelligence Accused of 'Spying on USA,'* Telegraph (June 22, 2017).[21] Surely, these same governments could send information to or receive information from the United States.

[20] Available at: https://www.aclu.org/blog/national-security/privacy-and-surveillance/us-intelligence-community-can-share-your-personal.

[21] Available at: https://www.telegraph.co.uk/news/2017/06/22/germany-accused-hypocrisy-claims-spied-usa/.

Governments have—and will—use their surveillance powers to spy on human rights defenders. As described below, the knowledge that HRW is a target of surveillance, whether prospectively or retrospectively, significantly impedes its important work.

B. Illegal Surveillance Makes HRW's Work More Difficult

The Government's unlawful mass surveillance places great strain on HRW, making it more difficult for HRW to fulfill its mission.

One of the most troubling aspects of U.S. government mass surveillance is that it is a black box. HRW employees said that they assume they are always being surveilled. They warned that the uncertainty can also lead people to be lulled into a false sense of security. Indeed, many HRW employees explained that they had not understood the dramatic scope of American surveillance until Edward Snowden's whistleblowing. Adding to this unknown, the Government has never delineated the parameters of its mass surveillance in any meaningful way—it is not even clear what legislative authority the Government claims is the source of its power to conduct the surveillance here. Plaintiffs' counsel explained in a joint hearing in this case and the case in which HRW is a plaintiff that it was "not at all clear that collection [of] telephone records is only happening under Section 215 of the PATRIOT Act" and, as a result, Plaintiffs' complaint addresses Defendants' conduct rather than their

rationale: "We didn't sue only about the collection that's happening under whatever hat the Government happens to be wearing this day. We sued about the collection of telephone records." Amended Transcript of Proceedings at 24:19–25:1, *First Unitarian Church of L.A. v. NSA*, No. 4:13-cv-03287-JSW (N.D. Cal. Mar. 20, 2014), ECF No. 101.

Perhaps wryly, one scholar claimed that Chinese Internet surveillance techniques are more consistent with international human rights norms at least in part because their application is more predictable—that is, unlike Chinese citizens, Americans believe that their Internet conduct might not be collected and examined by the Government without a warrant or reasonable suspicion. Chinese citizens, in contrast, expect such surveillance as a matter of course. *See* James D. Fry, *Privacy, Predictability and Internet Surveillance in the U.S. and China: Better the Devil You Know?*, 37 U. Pa. J. Int'l L. 419, 420–21, 481 (2015).

This uncertainty makes planning difficult. As HRW and the ACLU reported, "without a clear sense of the boundaries of US government surveillance, and the effectiveness of various countermeasures, it is difficult to discern what steps" might be taken to protect information. *With Liberty to Monitor All*, *supra*, at 57. The cloud of uncertainty forces HRW employees to take burdensome cautionary measures or prevents them from performing certain duties altogether.

1. Travel/In-Person Meetings

One way to reduce the likelihood of electronic surveillance is to communicate in person. *See, e.g.*, *With Liberty to Monitor All*, *supra*, at 35 ("Many journalists reported a strong preference for meeting sources in person in large part for reasons of security."). When HRW employees worked on *Delivered into Enemy Hands*, they worried about communicating securely with their sources because the sources were subject to retaliation. As a result, HRW and the sources frequently met in person. Another employee reported that she sometimes has face-to-face meetings where the participants leave cellular phones in a house and talk outside to get out of the range of the phones' microphones.

Similarly, one HRW employee stationed outside the United States explained that when HRW works with local lawyers in the Middle East or Africa, they usually can only communicate face-to-face in neutral third countries. Such meetings are both difficult to arrange without creating electronic records and much more costly than a simple phone call or email exchange, in terms of both time and money. Despite this, for many HRW employees, in-person meetings are a necessity and a matter of course.

2. Encryption

In addition to in-person meetings, another response to the danger of mass surveillance is encryption. Encryption occurs when a series of operations are used to

transform data into unreadable text. *See* Orin S. Kerr & Bruce Schneier, *Encryption Workarounds*, 106 Geo. L.J. 989, 993 (2018) ("For example, the algorithm might merely change each letter in the alphabet one letter so that A becomes B, B becomes C, C becomes D, and so on. . . . Modern encryption algorithms use the same principle but rely on complex mathematics."). When encryption is done properly, only a party with the "key" can "decrypt"—or reverse the steps taken to encrypt the data—and restore the original readable data. *See id.* at 993–94. Unlike the short passwords that everyday users employ for standard services, keys are designed to be too long to guess. *See id.* In many instances of encryption, the key or the protocols to generate the key are held by a third-party. "In such cases three entities (at least) can decrypt the communication: the sender, the recipient, and the third party that handled the key exchange." Alan Z. Rozenshtein, *Surveillance Intermediaries*, 70 Stan. L. Rev. 99, 136 (2018). By contrast, to minimize the risk of unlawful surveillance, HRW employees frequently use end-to-end encryption. With end-to-end encryption, "[o]nly the sender and the recipient (the 'ends' of the communication) can decrypt the message." *Id.* at 137.[22] When HRW employees use end-to-end encryption to talk to

[22] For an interactive explanation of how encryption can or cannot protect communications, see *Everyday Encryption*, Human Rights Watch, https://www.hrw.org/everyday-encryption (last visited Sept. 11, 2019).

subjects and sources, their message is more secure than when transmitted by other means because no third party knows the key.

But there are numerous problems with encryption. HRW employees explained that using even the most widely available end-to-end encryption tools slows HRW's work. For instance, many sources are unfamiliar with encryption and are put off by the difficulty in using the technology. *See also With Liberty to Monitor All*, *supra*, at 29 ("[I]t can be difficult to get casual contacts to take more elaborate security measures to communicate.").[23] As a result, some sources will not speak to HRW after HRW tries to have an encrypted conversation. And even when both parties are able to use encryption, it can still be hard, for instance, to initiate a conversation. And encryption can be difficult to employ in less developed countries where the Internet is not as stable.

[23] Social science shows that reminding individuals of surveillance programs chills their speech. For instance, one study concluded that "being primed of government surveillance significantly reduced the likelihood of speaking out in hostile opinion climates." Elizabeth Stoycheff, *Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring*, Journalism & Mass Media Comm. Q. 1, 12 (2016). Another story reported that "the Snowden revelations . . . triggered a measurable shift in the way people used the Internet." Jeff Guo, *New Study: Snowden's Disclosures About NSA Spying Had a Scary Effect on Free Speech*, Wash. Post (Apr. 27, 2016), *available at* https://www.washingtonpost.com/news/wonk/wp/2016/04/27/new-study-snowdens-disclosures-about-nsa-spying-had-a-scary-effect-on-free-speech/.

Some sources are also concerned that the use of encrypted messaging and other technologies could "draw[] more attention to" the source or the researcher. *With Liberty to Monitor All*, *supra*, at 33. For instance, one HRW employee worried that the Government might realize that a government-employed source had an encrypted communications app on his or her phone and then confiscate that phone. At that point, the Government could see all the encrypted messages: "If prosecutors get [a] source's phone, end-to-end encrypted texts are not necessarily going to help." Trevor Timm, *The Trump Administration's New Methods for Cracking Down on Leakers*, Colum. Journalism Rev. (Oct. 18, 2018).[24]

The necessary use of encrypted communication with third-party sources also makes HRW's work more difficult administratively. Encrypted communications with third-party sources frequently take place on low-cost or free services. As journalists reported to HRW and the ACLU, "[t]hey can take time to learn, and are often difficult to use. Journalists we spoke with characterized them as 'a burden,' 'a huge tax on your time,' and 'cumbersome and slow.'" *With Liberty to Monitor All*, *supra*, at 34 (footnotes omitted). One employee described such a service as "not very user

[24] Available at: https://www.cjr.org/politics/trump-leaker-arrest-natalie-mayflower-sours-edwards.php.

friendly." As a result, encrypted communications with third-party sources create unnecessary internal roadblocks within HRW.

These obstacles are especially frustrating because HRW is fundamentally an information-sharing enterprise. Its employees work hard to collect and share information in service of exposing and stopping human rights abuses. To do that effectively, they must be able to communicate and collaborate. Even though encryption services inhibit interoffice data sharing, requiring ad hoc workarounds, HRW employees are forced to use them to avoid illegal mass surveillance like the kind identified by Plaintiffs.

And, for all of the downsides to using encryption, it might not even work because, as described above, the Government's capabilities are unknown. Several HRW researchers told us they assume that encryption will not be fool-proof protection and they are cautious about recording identifying information even when using it.

3. Other Issues With Surveillance

Beyond these logistical hurdles, surveillance adds additional stress to HRW. One HRW advocate said that it makes him anxious "knowing that they have such huge capabilities to spy on people . . . . It gives me a lot of anxiety." HRW employees are concerned that any slip in security protocol could jeopardize an entire investigation. *See, e.g.*, *With Liberty to Monitor All*, *supra*, at 32 ("[O]ne lapse in

protecting encryption passphrases or hardware can provide others with direct access to sensitive data in unencrypted form."). Several employees similarly reported concern that the Government was surveilling their personal communications.

At the end of the day, every HRW employee interviewed said there was some information that they simply would not discuss through any means because of fear of surveillance and that this limited their research and ability to talk to their sources.

* * *

HRW employees who work with sensitive information have had to restructure the way they investigate and report. They must devote a large proportion of their time trying to avoid warrantless surveillance. Until individuals can challenge illegal surveillance, HRW's burdens will likely only grow. Even "secure" technologies are frequently found to be vulnerable. Abigail Ng, *It's Not Just WhatsApp, Most Messaging Apps Likely Have Security Vulnerabilities*, CNBC (May 21, 2019) (explaining that "it is 'literally impossible' to prove the absence of a vulnerability" in software).[25] For instance, the popular encrypted application WhatsApp has had several notable vulnerabilities reported. This year, news sources reported that a vulnerability allowed third-parties to spy on users' phones through WhatsApp and that WhatsApp

[25] Available at: https://www.cnbc.com/2019/05/22/whatsapp-messaging-app-cybersecurity-vulnerability.html.

had blocked an attack on a "UK-based human rights lawyer." Thomas Ricker, *Update WhatsApp Now to Avoid Spyware Installation from a Single Missed Call*, The Verge (May 14, 2019).[26]

And the Government's surveillance capabilities are constantly growing. Among other things, the NSA "vacuumed up more than 534 million records of phone calls and text messages from American telecommunications providers like AT&T and Verizon last year—more than three times what it collected in 2016." Charlie Savage, *N.S.A. Triples Collection of Data From U.S. Phone Companies*, N.Y. Times (May 4, 2018).[27] One HRW employee said that whenever a new vulnerability is announced, he and others discuss how to respond and implement more training to increase security. These challenges force HRW employees to try to adapt to a constantly changing technical landscape, diverting time and resources away from HRW's core human rights mission.

[26] Available at: https://www.theverge.com/2019/5/14/18622744/whatsapp-spyware-nso-pegasus-vulnerability.

[27] Available at: https://www.nytimes.com/2018/05/04/us/politics/nsa-surveillance-2017-annual-report.html.

II. WHEN THE DISTRICT COURT'S RULING IS VIEWED IN THE CONTEXT OF "PARALLEL CONSTRUCTION," IT IS CLEAR THAT NO ONE WILL BE ABLE TO CHALLENGE UNLAWFUL SURVEILLANCE IN COURT

Beyond allowing the Government's unlawful surveillance to continue taxing HRW's important work in the significant ways described above, the district court's ruling will have dire consequences for the persistence of illegal surveillance at large. In particular, the district court's holding that state secrets precluded the court even from ruling as to Plaintiffs' ability to challenge the surveillance program in this case effectively insulates surveillance from judicial review under any circumstances.

The district court held that Plaintiffs do not have standing because state secrets would have to be disclosed to determine whether Plaintiffs had been surveilled: "[E]ven a simple 'yea or nay' as to whether Plaintiffs have standing to proceed on their statutory claims would do grave harm to national security." ER026:3–5. Under that logic, unlawful surveillance could be challenged only by individuals that the Government admitted to surveilling. And, generally, the Government only admits to surveilling individuals when it uses evidence from surveillance against them in court. Even then, the Government can avoid admitting that any evidence was derived from surveillance. Through a deceptive tactic called "parallel construction," the Government encourages law enforcement to discover the evidence through alternate forms of search and conceals the role that surveillance played in the prosecution.

Parallel construction and willful nondisclosure of surveillance prevents accused criminals from learning about surveillance, without which they cannot challenge unlawful surveillance in court. This is key background when considering the district court's ruling; if that decision is upheld, virtually no one could challenge illegal warrantless surveillance even while everyone suffered concrete, particularized injuries.

A. The District Court's Holding Bars Everyday Americans From Challenging Unlawful Surveillance In Court

As Plaintiffs explain in their opening brief (*see* Opening Br. 14–64), the district court's ruling misapplies the law of standing. The district court held that Plaintiffs do not have standing because, essentially, the Government refused to agree they had standing. For instance, the district court refused to accept whistleblower Edward Snowden's authentication of a draft NSA Inspector General report, stating, "Defendants do not authenticate the exhibit. . . . Further, there has been no waiver of the state secret privilege over the document and Defendants have objected on the basis of the privilege to Plaintiffs' requests for admissions regarding the authenticity of this document." ER019:8–22.

More broadly, the district court concluded that the state secrets privilege would prevent plaintiffs from showing standing under any set of evidence because of the risk of disclosure of state secrets: "[E]ven if the public evidence proffered by Plaintiffs

were sufficiently probative to establish standing, ***adjudication of the standing issue could not proceed without risking exceptionally grave damage to national security***." ER020:13–15 (emphasis added); *see also* ER053:25–27 (same). At the end of the day, "the Court accept[ed] the representation of the Defendants that they are unable to defend the litigation or to pursue it to resolution on the merits without grave risk to the national security." ER009:11–13.

Under this reasoning, no plaintiff whom the Government did not admit to surveilling would ever have standing.

B. Parallel Construction Prevents Criminal Defendants From Challenging Unlawful Surveillance In Court

The district court has, in effect, shut the courthouse door to ordinary Americans like Carolyn Jewel whom the Government will not admit to surveilling. Instead, the only individuals who would have standing to challenge unlawful government mass surveillance would be criminal defendants informed by the Government that they were surveilled. But the Government frequently avoids providing that information to accused criminals—even though their constitutionally protected liberty is at stake—by using "parallel construction."

Under parallel construction, after the Government obtains evidence against an alleged criminal from a surveillance program, it then takes steps to reconstruct that

evidence through other means.[28] For instance, the Drug Enforcement Agency would learn through secret surveillance that drugs were being smuggled in a particular automobile and then tip off federal agents to stop that person without explaining the basis of the DEA's "recommendation." Then, as one agent reported, "You'd be told only, 'Be at a certain truck stop at a certain time and look for a certain vehicle.' And so we'd alert the state police to find an excuse to stop that vehicle, and then have a drug dog search it." John Shiffman & Kristina Cooke, *Exclusive: U.S. Directs Agents to Cover Up Program Used to Investigate Americans*, Reuters (Aug. 5, 2013).[29]

Following these revelations about the widespread use of parallel construction, HRW engaged in a detailed investigation for more than eighteen months that resulted in an in-depth report, *Dark Side*. (The name of the report is derived from the nickname

[28] The extensive use of parallel construction to shield surveillance from the judicial system was revealed by Reuters, which described how the U.S. Drug Enforcement Agency's Special Operations Division "distribut[es] tips from overseas NSA intercepts, informants, foreign law enforcement partners and domestic wiretaps" to law enforcement officers on the condition that the law enforcement officers not disclose SOD's involvement. John Shiffman & Kristina Cooke, *Exclusive: U.S. Directs Agents to Cover Up Program Used to Investigate Americans*, Reuters (Aug. 5, 2013), *available at* https://www.reuters.com/article/us-dea-sod/exclusive-u-s-directs-agents-to-cover-up-program-used-to-investigate-americans-idUSBRE97409R20130805.

[29] Available at: https://www.reuters.com/article/us-dea-sod/exclusive-u-s-directs-agents-to-cover-up-program-used-to-investigate-americans-idUSBRE97409R20130805.

of the Drug Enforcement Administration's Special Operations Division, suggesting that those involved have "doubts about the legality of [its] operations." *Dark Side*, *supra*.) In the report, HRW "identified numerous federal and state judicial decisions in which the government has admitted, after the fact, to having carried out what are known as 'whisper,' 'wall,' 'walled off,' or 'wall off' stops." *Id.*[30] Parallel construction is not an exception; it is "a law enforcement technique [the DEA] use[s] every day." Shiffman & Cooke, *supra*. And it "has grown in use in recent years." Amanda Claire Grayson, Note, *Parallel Construction: Constructing the NSA Out of Prosecutorial Records*, 9 Harv. L. & Pol'y Rev. Online S25, S33 (2015).

The Government has argued that this "laundering" of the evidence means that it need not disclose details about the original surveillance as part of the prosecution. Shiffman & Cooke, *supra*; *see also Responsive Documents*, MuckRock (Feb. 3, 2014) ("'[P]arallel construction' can shield information that might otherwise be

[30] The pretextual stops themselves are not new. *See, e.g.*, California Legislature Task Force on Government Oversight, *Operation Pipeline* (1999), *available at* https://web.archive.org/web/20010127120300/http://www.aclunc.org/discrimination/webb-report.html (describing the "troubling legal and ethical questions" surrounding "'whisper stops' or 'wall cases'"). What is new is pairing these pretextual stops with the increased breadth of warrantless, mass surveillance and the related increase in the frequency of the use of parallel construction.

discoverable . . . .").[31] HRW surveyed cases in which parallel construction was challenged and learned that the Government makes standard arguments in response to attempts to learn about surveillance evidence: (i) that the defendant is speculating or going on a fishing expedition; (ii) that any evidence is not relevant or discoverable; (iii) that the prosecution team does not possess the evidence; and (iv) that the government will not use the underlying surveillance as evidence. *See Dark Side*, *supra*. In rare instances when the Government's efforts to conceal surveillance are unsuccessful, it can simply dismiss the case to avoid disclosing any surveillance. As former Office of the Director of National Intelligence general counsel Robert Litt told HRW, "[I]f the Intelligence Community says, 'You can't risk this information, you need to dismiss the case,' that carries the day[.]" *Dark Side*, *supra*.

As HRW explained, the purpose of parallel surveillance is "***to keep an investigative activity hidden from courts and defendants—and ultimately from the public***." *Dark Side*, *supra* (emphasis added). Indeed, "[u]sing parallel construction is no doubt a deliberate attempt to bypass constitutional guarantees that undermine procedures for fairness and accountability." Natasha Babazadeh, *Concealing Evidence: "Parallel Construction," Federal Investigations, and the Constitution*, 22

[31] Available at: https://www.documentcloud.org/documents/1011382-responsive-documents.html#document/p134.

Va. J.L. & Tech. 1, 57 (2018). Not only does parallel construction allow the Government to avoid public disclosure and judicial scrutiny of its use of surveillance in individual instances, but it likely uses parallel construction "to hide [entire] intelligence surveillance ***programs***," which means that "wide-ranging or acute civil liberties violations may go unnoticed." *Dark Side*, *supra* (emphasis added).

Even the Department of Justice has recognized that it may be using parallel construction unlawfully. In March 2019, the Department of Justice Office of Inspector General issued a report on the Drug Enforcement Agency's use of administrative subpoenas to collect or exploit bulk data. That report touched on the DEA's troubling use of parallel surveillance to prevent prosecutors from becoming aware of surveillance information that they must disclose:

> [P]arallel construction should not be used to prevent prosecutors from fully assessing their discovery and disclosure obligations in criminal cases. While the DEA has denied misusing parallel construction in this manner, we found some troubling statements in the DEA's training materials and other documents, including that Program A investigative products cannot be shared with prosecutors. Such statements appear to be in tension with Department policy on a federal prosecutor's "duty to search" for discoverable information . . . .

A Review of the Drug Enforcement Administration's Use of Administrative Subpoenas to Collect or Exploit Bulk Data, at iv, U.S. Department of Justice Office of Inspector

General (Mar. 2019).[32] While the report noted that parallel construction was "beyond the scope of this review," it recommended "a comprehensive review by those DOJ components with expertise in this area." *Id.* at 122–23.

Similarly, leaders of both major political parties recognize that parallel surveillance is objectionable. As U.S. Senator Rand Paul opined, "the government should be disallowed from taking [warrantless surveillance] information and developing a parallel construction of a case, where the illegally obtained information is not used in court but is used by law enforcement to develop other information to mount a prosecution." Rand Paul, *No Foreign Spy Program Reauthorization Without Citizen Protections*, Reason (Jan. 2, 2018);[33] S. 1997, 115th Cong. § 6 (2017).

Recent history confirms the Government cannot be trusted to decide unilaterally whether to disclose surveillance, as parallel construction allows it to do. In 2012, the Government told the Supreme Court that it would notify criminal defendants about the use of certain surveillance data against them. The Solicitor General learned this was false, and ultimately convinced the Government to provide notice. But the Government notified fewer than ten individuals, some of whom could not actually

[32] Available at: https://oig.justice.gov/reports/2019/o1901.pdf.

[33] Available at: https://reason.com/2018/01/02/no-foreign-spy-program-reauthorization-w.

challenge the surveillance because, for instance, they had already accepted plea bargains. *See* Patrick Toomey & Brett Max Kaufman, *The Notice Paradox: Secret Surveillance, Criminal Defendants, & the Right to Notice*, 54 Santa Clara L. Rev. 843, 868–72 (2014). In another example, the Government engaged in a surveillance program known as the "Terrorist Surveillance Program" beginning in 2001, but did not disclose its existence even to most members of Congress until 2005. *See* S. Rep. 110-209, at 4 (2007).

In sum, the Government takes pains to conceal surveillance from everyone, including criminal defendants to whom the Government has a legal duty to disclose incriminating evidence.

Nevertheless, in this case, the district court held that everyday Americans do not have standing because the Government would not concede it was surveilling them. This incentivizes the Government to expand its use of parallel surveillance. Moreover, because the Government employs parallel construction to avoid disclosing illegal surveillance to criminal defendants, they cannot challenge surveillance either. The district court's ruling thus bars virtually everyone from reaching the merits. The Government's use of parallel construction further increases the need for citizens like

Carolyn Jewel and her co-plaintiffs to be allowed to pursue their legal challenge to the unlawful surveillance at issue in this case.[34]

CONCLUSION

For these reasons, the district court's decision allowing sweeping government surveillance to proceed without judicial review is dangerous and should be reversed.

[34] *See, e.g.*, Randy Barnett, *Why the NSA Data Seizures Are Unconstitutional*, 38 Harv. J.L. & Pub. Pol'y 3, 19 (2015) (explaining that when plaintiffs do not have standing, there is no public assessment of surveillance programs' constitutionality and it is "impossible to hold elected officials and appointed bureaucrats accountable").

Dated: September 13, 2019

Respectfully submitted,

WILSON SONSINI GOODRICH & ROSATI
Professional Corporation

By: *s/ Brian M. Willen*

Brian M. Willen
Brian J. Levy
1301 Avenue of the Americas
40th Floor
New York, NY 10019
Telephone: (212) 999-5800
Facsimile: (212) 999-5899
Email: bwillen@wsgr.com; blevy@wsgr.com

Lauren Gallo White
Kevin Laxalt-Nomura
One Market Plaza
Spear Tower, Suite 3300
San Francisco, CA 94105
Telephone: (415) 947-2000
Facsimile: (415) 947-2099
Email: lwhite@wsgr.com; knomura@wsgr.com

Counsel for Amicus Curiae

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

Form 8. Certificate of Compliance for Briefs

Instructions for this form: http://www.ca9.uscourts.gov/forms/form08instructions.pdf

9th Cir. Case Number(s) 19-16066

I am the attorney or self-represented party.

This brief contains 6,988 **words**, excluding the items exempted by Fed. R. App. P. 32(f). The brief's type size and typeface comply with Fed. R. App. P. 32(a)(5) and (6).

I certify that this brief *(select only one)*:

- ○ complies with the word limit of Cir. R. 32-1.
- ○ is a **cross-appeal** brief and complies with the word limit of Cir. R. 28.1-1.
- ◉ is an **amicus** brief and complies with the word limit of Fed. R. App. P. 29(a)(5), Cir. R. 29-2(c)(2), or Cir. R. 29-2(c)(3).
- ○ is for a **death penalty** case and complies with the word limit of Cir. R. 32-4.
- ○ complies with the longer length limit permitted by Cir. R. 32-2(b) because *(select only one):*
  - ○ it is a joint brief submitted by separately represented parties;
  - ○ a party or parties are filing a single brief in response to multiple briefs; or
  - ○ a party or parties are filing a single brief in response to a longer joint brief.
- ○ complies with the length limit designated by court order dated _____.
- ○ is accompanied by a motion to file a longer brief pursuant to Cir. R. 32-2(a).

Signature s/Brian M. Willen **Date** 09/13/2019

*(use "*s/[typed name]*" to sign electronically-filed documents)*

Feedback or questions about this form? Email us at forms@ca9.uscourts.gov