Nos. 20-1119, 20-1311

IN THE

UNITED STATES COURT OF APPEALS

FOR THE FOURTH CIRCUIT

Anas Elhady et al.,

Plaintiffs-Appellees,

v.

Charles H. Kable IV, Director of the Terrorist Screening Center, in his official capacity, et al.,

Defendants-Appellants.

On appeal from the United States District Court
for the Eastern District of Virginia
Case No. 1:16-cv-00375-AJT-JFA
Hon. Anthony J. Trenga

PAGE PROOF BRIEF OF AMICUS CURIAE ELECTRONIC FRONTIER FOUNDATION IN SUPPORT OF PLAINTIFFS-APPELLEES

Matthew Borden
Athul K. Acharya
Gunnar Martz
BRAUNHAGEY & BORDEN LLP
351 California Street, 10th Fl.
San Francisco, CA 94104
(415) 599-0210

Saira Hussain
Mark Rumold
Kit Walsh
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
(415) 436-9333

Counsel for Amicus Curiae

June 2, 2020

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

CASES

RULES

STATEMENT OF INTEREST[1]

Amicus curiae the Electronic Frontier Foundation (EFF) is a member-supported, non-profit civil liberties organization that has worked for nearly thirty years to ensure that technology supports freedom, justice, and innovation for all the people of the world. With over 30,000 members, EFF represents the interests of those impacted by new technologies both in court cases and in broader policy debates, and actively encourages and challenges the government and courts to support privacy and safeguard individual autonomy to ensure that new technology enhances civil liberties rather than abridges them.

This case directly implicates EFF's mission of promoting government transparency and protecting electronic privacy and free speech. Individuals in the federal government's Terrorist Screening Database ("the Watchlist") find their rights to travel, privacy, and free speech infringed with minimal process—without even knowledge of their inclusion in the database. As an organization dedicated to protecting such rights, EFF has unique insight into the stigma and harms caused by the government's conduct, which will help inform this Court's decision.

[1] No counsel for a party authored this brief in whole or in part, and no person other than *amicus* or their counsel has made any monetary contributions to fund the preparation or submission of this brief. All parties have consented to the filing of this brief.

INTRODUCTION

The government has surreptitiously placed over one million United States citizens and foreign nationals on the Watchlist based on a malleable standard that considers their race, religion, national origin, and First Amendment activities. This Watchlist is distributed over countless government networks and follows those included wherever they go, like an indelible digital mark of Cain.

By putting someone on the Watchlist, the government brands that person a terrorist. It promulgates its assessment to tens of thousands of federal agencies, state and local police departments, private security forces, and foreign governments. As one court put it, once a person is on the Watchlist, that designation "propagate[s] extensively through the government's interlocking complex of databases, like a bad credit report that will never go away." *Ibrahim v. Dep't of Homeland Sec.*, 62 F. Supp. 3d 909, 928 (N.D. Cal. 2014).

People on the Watchlist are seized and searched at length, often at gunpoint. They suffer longer, more intrusive, and more dangerous encounters with law enforcement at every level of government. They are denied immigration benefits and economic opportunities. And those are just the intended effects. Because of the low standard for inclusion on the Watchlist, it is more prone to erroneous information than most databases. And because it is a secret, those it afflicts can never even *know* they are on it, let alone petition effectively to be removed.

All this amounts to an invasion of a protected liberty interest under the Supreme Court's "stigma plus" test. Being labeled a known or suspected terrorist is stigmatic. And being on the Watchlist inflicts severe harm on people in their everyday lives. For the reasons below, this Court should hold that Plaintiffs have satisfied the elements of a stigma-plus claim.

SUMMARY OF ARGUMENT

Under the Supreme Court's stigma-plus test, the government infringes a protected liberty interest when it harms a person's reputation and alters their rights or legal status. *Paul v. Davis*, 424 U.S. 693, 711-12 (1976); *Cannon v. Vill. of Bald Head Island*, 891 F.3d 489, 501 (4th Cir. 2018). The federal government does both when it puts people on the Watchlist. It harms their reputations by branding them terrorists and broadcasting that accusation to tens of thousands of government agencies across the country and around the world. And it alters their rights or legal status in countless ways, including by:

- Enlisting state and local law enforcement to seize such persons for longer, search them more thoroughly, and deliver any information discovered back to the federal government;
- Directing its own agencies to search and copy such persons' electronic devices at the border, and advising state and local agencies to do the same in the interior;
- Denying immigration benefits to such persons by default, including supposedly nondiscretionary benefits like naturalization;
- Preventing such persons from obtaining jobs that require travel or certain licenses; and
- Putting their personal data at risk of misuse by government officials or breach by malicious outsiders.

Each of these, on its own, would be enough to show that the government has altered the rights or status of persons on the Watchlist. Taken together, Plaintiffs have amply proven the elements of a stigma-plus claim.

ARGUMENT

When the government harms a person's reputation and alters their rights or legal status, it trenches upon the liberty protected by the Due Process Clause. *Paul*, 424 U.S. at 711-12. A due process claim for reputational harm has two elements: (1) that the government "placed a stigma on [the plaintiff's] reputation" and (2) that the government "'distinctly altered or extinguished' [the plaintiff's] legal status." *Cannon*, 891 F.3d at 501; *Shirvinski v. U.S. Coast Guard*, 673 F.3d 308, 315 (4th Cir. 2012) (quoting *Paul*, 424 U.S. at 711). This test is known as the "stigma plus" test. *Ridpath v. Bd. of Governors Marshall Univ.*, 447 F.3d 292, 309 n.16 (4th Cir. 2006).

By putting people on the Watchlist, the government brands them as terrorists. It diminishes or extinguishes many of their rights and distinctly alters their legal status. For people on the Watchlist, routine encounters with law enforcement become fraught confrontations. Immigration benefits, including nondiscretionary ones like naturalization, become nearly impossible to obtain. Fourth Amendment protections seem to apply with diminished force. And many other harms abound, including loss of employment and other economic opportunities.

I. BRANDING SOMEONE A "TERRORIST" AND SHARING THAT INFORMATION SATISFIES THE STIGMA REQUIREMENT

On the basis of nothing more than reasonable suspicion of conduct "related to terrorism"—a vague and overbroad standard that snares all manner of innocent people—the government can put someone on the Watchlist and label them a terrorist. It then disseminates that determination far and wide—not only to the federal agencies tasked with maintaining national security, but also to tens of thousands of state, local, tribal, and territorial governments, as well as private security forces and foreign countries. In so doing, the government brands those on the Watchlist with a constitutionally cognizable stigma.

A. Being branded a terrorist is highly stigmatizing

Courts have recognized a wide variety of statements and imputations that satisfy the "stigma" element of the stigma-plus test. Suggesting that someone is a criminal is sufficiently stigmatic for purposes of due process. *See Paul*, 424 U.S. at 697. So are charges of harassment, dishonesty, and immorality. *See Cannon*, 891 F.3d at 502; *Ridpath*, 447 F.3d at 308-09. Branding someone a terrorist is at least as bad as any of these.

The government does not dispute that putting someone on the Watchlist, and thereby deeming them a known or suspected terrorist, is stigmatizing. *See* Opening Br. 42-46. Yet the bar is quite low for the government to brand someone with this modern-day scarlet letter: a "suspected terrorist" is anyone who

> is reasonably suspected to be, or has been, engaged in conduct constituting, in preparation for, in aid of, or related to terrorism and/or terrorist activities based on articulable and reasonable suspicion.[2]

Oversight agencies within the government itself have recognized that "determining whether individuals meet these minimum standards can involve some level of subjectivity."[3] In determining that a person meets this vague standard, an agency is allowed to consider protected characteristics, such as the person's race, ethnicity, religious affiliation, and First Amendment activities. JA __ [Dkt. 323 at 5]. Moreover, the government can exempt itself from even this low bar "as needed," even if "the exception is cloaked in state secrets." *Ibrahim*, 62 F. Supp. 3d at 930.

Yet, relying on this thinnest of reeds, the government has deemed more than 1.2 million people known or suspected terrorists and put them on the Watchlist. JA __ [Dkt. 323 at 4]. By the government's own reckoning, however, more than 40 percent of people on the Watchlist have "[n]o recognized terrorist group affiliation."[4] Even when an individual

---

[2] Jerome P. Bjelopera et al., *The Terrorist Screening Database and Preventing Terrorist Travel*, Congressional Research Serv. 4 (Nov. 7, 2016), https://fas.org/sgp/crs/terror/R44678.pdf.

[3] Gov't Accountability Office, GAO-08-110, *Terrorist Watch List Screening: Opportunities Exist to Enhance Management Oversight, Reduce Vulnerabilities in Agency Screening Processes, and Expand the Use of the List* 18 (Oct. 2007).

[4] *Tide By the Numbers*, National Counterterrorism Center (Aug. 2013), https://cdn.arstechnica.net/wp-content/uploads/2014/08/TIDE_by_the_numbers.jpg. *See also* Cyrus Farivar, *Nearly half of US terror suspects "not connected" to known groups*, Ars Technica (Aug. 5,

successfully defends against a terrorism-related criminal charge, they may remain on the Watchlist.[5] Thus, not only is being on the Watchlist stigmatizing, it is often unjustified.

Nevertheless, most nominations to the Watchlist are accepted—from 2009 to 2013, only one percent of nominations were rejected.[6] And getting off the Watchlist is extremely difficult. The government provides a modicum of process through the U.S. Department of Homeland Security (DHS) Traveler Redress Inquiry Program (TRIP), but people who use it are never told whether they are on the Watchlist, why they might be on the Watchlist, or whether they have been removed from the Watchlist. JA ___ [Dkt. 308-12 at 9-10]. At best, it results in "Kafkaesque on-off-on-list treatment" without any real relief. *Ibrahim*, 62 F. Supp. 3d at 931.

B. Accusations of terrorism are stigmatizing when shared with other government agencies

Harms to an individual's reputation need not be broadly and publicly disseminated to be stigmatizing. This Court has held that a plaintiff need not even show "a specific instance of actual dissemination" to prove a stigma-plus claim. *Sciolino v. City of Newport News*, 480 F.3d 642, 648

2014), https://arstechnica.com/tech-policy/2014/08/nearly-half-of-us-terror-suspects-not-connected-to-known-groups/.

[5] Charlie Savage, *Even Those Cleared of Crimes Can Stay on F.B.I.'s Watch List*, N.Y. Times (Sep. 27, 2011), https://www.nytimes.com/2011/09/28/us/even-those-cleared-of-crimes-can-stay-on-fbis-terrorist-watch-list.html.

[6] Bjelopera, *supra* note 2, at 6.

n.4, 649 (4th Cir. 2007). Harmful assertions are stigmatic if they are "availab[le] upon request" and there is a "likelihood" that someone will inspect them. *Cannon*, 891 F.3d at 503-04 (citing *Sciolino*, 480 F.3d at 646-50); *Ledford v. Delancey*, 612 F.2d 883, 885-87 (4th Cir. 1980). The same rule holds in other circuits. *See, e.g.*, *Dupuy v. Samuels*, 397 F.3d 493, 511-12 (7th Cir. 2005) (information sufficiently disclosed if "available to any federal agency"); *Doe v. U.S. Dep't of Justice*, 753 F.2d 1092, 1113 (D.C. Cir. 1985) (information sufficiently disclosed if "available to prospective employers or other government personnel").

Nor must the information be *publicly* available—availability to other government agencies, both within and across sovereigns, suffices. In *Shirvinski*, for example, this Court held that if the government had excluded the plaintiff from operating as a government contractor in the future—i.e., if it had just communicated his unsuitability *within* the government—the plaintiff would have stated a claim. 673 F.3d at 315-16. Similarly, the D.C. Circuit has held that "communicat[ion] to other government agencies" is sufficient disclosure. *Doe*, 753 F.2d at 1111. So have the Seventh and Ninth Circuits. *Dupuy*, 397 F.3d at 511-12 (communication to "any federal agency"); *Humphries v. Cty. of Los Angeles*, 554 F.3d 1170, 1175-76, 1188 (9th Cir. 2009) (communication to

"a broad array of government agencies, employers, and law enforcement entities"), *rev'd on other grounds*, 562 U.S. 29 (2010).[7]

The government does not dispute that it broadcasts the Watchlist to over 18,000 law enforcement agencies at all levels of federal, state, local, and tribal governments, as well as another 533 private entities. JA __ [Dkt. 323 at 7]. Instead, it argues that disclosure does not count because it is "not made broadly to the public." Opening Br. 43-44. For the reasons discussed above, that argument is contrary to the law of this Court and the majority of the courts of appeal. *Sciolino*, 480 F.3d at 648 n.4, 649; *see, e.g.*, *Doe*, 753 F.2d at 1111; *Dupuy*, 397 F.3d at 511-12; *Humphries*, 554 F.3d at 1175-76, 1188.

Disclosure to 18,000 law enforcement agencies is more than enough to place a "constitutionally cognizable stigma" on the reputations of those on the Watchlist. *See Cannon*, 891 F.3d at 503.

II. PEOPLE ON THE WATCHLIST SUFFER NUMEROUS "PLUS" FACTORS, INCLUDING DEPRIVATION OF LEGAL RIGHTS AND PHYSICAL AND ECONOMIC HARMS

Under the stigma-plus test, in addition to stigma, the government must alter or extinguish some right or legal status. This is the "plus" requirement. *Shirvinski*, 673 F.3d at 315 (quoting *Paul*, 424 U.S. at 711).

---

[7] The Supreme Court reversed *Humphries* on the limited issue of prospective relief against Los Angeles County. *Los Angeles Cty. v. Humphries*, 562 U.S. 29, 33-34 (2010). It did not disturb the Ninth Circuit's decision in any respect relevant to this case. *Humphries v. Cty. of Los Angeles*, 649 F.3d 1077 (9th Cir. 2011).

Any alteration or diminution of an individual's legal rights or status, no matter how slight, suffices.

The "plus" standard is easily satisfied here for many separate and independent reasons. Those on the Watchlist suffer more dangerous and intrusive encounters with law enforcement, enhanced screening and secondary inspection when flying or crossing the border, denial of immigration benefits, economic harms, and more. Any of these, standing alone, would be enough to alter or extinguish a right or legal status; taken together, they are more than enough to satisfy the stigma-plus test.

A. A "plus" factor is any government action that alters a person's legal rights or status

The government creates a "plus" factor when it "'distinctly alter[s] or extinguish[es]'" an individual's legal status. *Shirvinski*, 673 F.3d at 315 (quoting *Paul*, 424 U.S. at 711). The alteration need not be dramatic. In *Ridpath*, for example, this Court held that reassigning a government employee "to a position outside his field of choice"—even with a significant pay increase—was enough. 447 F.3d at 309-11. The government need not "effectively foreclose" exercise of a right or status to create a "plus"; it need only "*impair[]*" the right or status. *Cannon*, 891 F.3d at 502-03 (quoting *Ledford*, 612 F.2d at 885-87) (emphasis added in *Cannon*). Similarly, other circuits require only a "tangible burden" on an individual's ability to obtain a right or status. *Valmonte v. Bane*, 18 F.3d 992, 1001 (2d Cir. 1994) ("tangible burden" on an individual's employment

prospects); *Humphries*, 554 F.3d at 1188 (same); *Dupuy*, 397 F.3d at 511-12 ("tangible loss" when commission's findings of alcoholism were "available to any federal agency"); *Doe*, 753 F.2d at 1108-09 ("some tangible change of status vis-a-vis the government").

Similarly, to constitute a "plus" factor, the harm to a plaintiff's rights or legal status need not be mandatory. In *Humphries*, for instance, the plaintiffs had been falsely accused of child abuse and placed on a register of child abusers. 554 F.3d at 1180-82. State law required some state agencies to check the register before granting rights or benefits. *Id.* at 1187-88. If an agency found an applicant on the register, however, it was not required to deny the right or benefit, but merely to investigate and draw its own "independent conclusions." *Id.* (quotation marks omitted). Thus, being on the register did not "fully extinguish" anyone's rights or status. *Id.* Still, the court held that because being on the register placed a "tangible burden" on the plaintiffs' ability to exercise rights or receive benefits, the state had sufficiently "altered" their status under *Paul*. *Id.* (pointing out that stigma-plus applies "when a right or status is 'altered *or* extinguished'" (quoting *Paul*, 424 U.S. at 711) (emphasis added in *Humphries*)). Thus, the "plus" factor is routinely established where the entities receiving stigmatizing information have some discretion about what to do with it. *See Cannon*, 891 F.3d at 502-03; *Dupuy*, 397 F.3d at 511-12; *Doe*, 753 F.2d at 1108-09; *Humphries*, 554 F.3d at 1188; *Valmonte*, 18 F.3d at 1001.

B. Being put on the Watchlist satisfies the "plus" test for at least five separate and independent reasons

When a person is labeled a known or suspected terrorist, their entire life changes. Routine traffic stops become more difficult and more dangerous. A person's electronic devices are more likely to be searched and copied both within the interior and at the border. Immigration benefits become nearly impossible to obtain. Securing credit and employment becomes harder. Personal data becomes more vulnerable to misuse or breach. Yet, because of the Watchlist's secrecy, an individual may never know that these changes result from their designation on the Watchlist. Each of these—and certainly all of them together—amounts to a change in legal status and diminishment in legal rights.

1. Encounters with law enforcement become longer, more difficult, more intrusive, and more dangerous

The Fourth Amendment's right against unreasonable seizures forbids police from detaining individuals for longer than "the time needed to handle the matter for which the stop was made." *Rodriguez v. United States*, 575 U.S. 348, 350 (2015). In *Rodriguez*, police stopped a car for driving on a highway shoulder, but then extended the stop by "seven or eight minutes" to run a drug-dog sniff. *Id.* at 351-52. The Supreme Court held that prolonging the stop beyond its initial purpose, even by a few minutes, violated the defendant's Fourth Amendment rights. *Id.* at 356-58. This Court has applied *Rodriguez* in similar circumstances. *See United States v. Bowman*, 884 F.3d 200, 219 (4th Cir. 2018).

Putting a person on the Watchlist impairs this right: officers often extend traffic stops based solely on Watchlist status. When the police pull someone over, they query the driver's name against several law-enforcement databases, including the Watchlist.[8] If a driver is listed in the Watchlist, the system "will pop up and say call the Terrorist Screening Center. . . . So now the officer on the street knows he may be dealing with a known or suspected terrorist."[9]

At that point, almost all police protocols direct a longer and more intrusive stop than might otherwise take place. For example:

- Baltimore instructs its police to "[u]se extreme caution when approaching and conversing with the individual" and to "immediately request back-up units." JA __ [Plaintiffs' MSJ Ex. 56 at 1-2]. For some individuals on the Watchlist, officers are instructed to remove them from the car, call a bomb unit, and deny them access to the car. *Id.* at 3. Even if cleared by the

[8] *See* U.S. Senate Permanent Subcommittee on Investigations, *Federal Support for and Involvement in State and Local Fusion Centers* 43-44 (Oct. 3, 2012), https://www.hsgac.senate.gov/imo/media/doc/10-3-2012%20PSI%20STAFF%20REPORT%20re%20FUSION%20CENTERS.2.pdf.

[9] Jeremy Scahill & Ryan Devereaux, *The Secret Government Rulebook for Labeling You a Terrorist*, The Intercept (July 23, 2014), https://theintercept.com/2014/07/23/blacklisted/ (quoting Tim Healy, the former director of the Federal Bureau of Investigation's Terrorist Screening Center).

bomb unit, officers are told to call DHS and not to release the individual until cleared by DHS. *Id.*

- Similar procedures in Michigan turned a simple traffic stop into a five-car back-up call, a 30-minute search and seizure, an arrest, and a prosecution—even though the man was ultimately convicted only of careless driving.[10]

Similarly, when someone on the Watchlist is arrested for unrelated reasons, being on the Watchlist can prolong the time they spend in custody or result in other complications:

- In New York, a criminal defendant who was set to be released on his own recognizance—the prosecution had not even sought bail—was abruptly remanded into custody when the judge noticed a Watchlist notation on his rap sheet. Neither the defendant's name nor his ethnicity matched those in the Watchlist notation; the only data that matched was the date of birth. After spending several extra hours in jail, the defendant was released without explanation.[11]

---

[10] Martin de Bourmont & Jana Winter, *Exclusive: FBI document reveals local and state police are collecting intelligence to expand terrorism watch list*, Yahoo! News (Feb. 7, 2020), https://news.yahoo.com/exclusive-fbi-document-reveals-local-and-state-police-are-collecting-intelligence-to-expand-terrorism-watch-list-100017370.html.

[11] Alex Kane, *Terrorist Watchlist Errors Spread to Criminal Rap Sheets*, The Intercept (Mar. 15, 2016),

- A man with a common Muslim name was arrested in the Bronx for driving while intoxicated. The man had no criminal record but did have a Watchlist notation on his rap sheet. The date of birth and the last name were a match, but the first name was not. Nevertheless, the police held his car for two months—purportedly as "evidence" for the intoxicated-driving case. In reality, the assistant district attorney wanted "to check with the feds in case they need to make sure there's no bomb in the car or something." For two months, being on the Watchlist meant the man had no car, which he needed to get to his job. Ultimately, the state released the car and the man pleaded guilty to a noncriminal traffic infraction.[12]

Encounters like these are common. A 2019 FBI report shows that 3,600 similar encounters took place over the previous two years, with at least one in every state, including Hawaii and Alaska.[13]

---

https://theintercept.com/2016/03/15/terrorist-watchlist-errors-spread-to-criminal-rap-sheets/.

[12] *Id.*

[13] FBI, *US Law Enforcement Encounters of Watchlisted Individuals Almost Certainly Yield Opportunities for Intelligence Collection, Enhancing US Government Knowledge of Threat Actors* (Oct. 23, 2019), https://www.scribd.com/document/445400976/FBI-Watchlist.

2. Electronic devices are more likely to be searched and seized

As the Supreme Court has recognized, electronic devices like cell phones are "not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans the privacies of life." *Riley v. California*, 573 U.S. 373, 403 (2014) (quotation marks and citation omitted). Indeed, "individuals store much more personal information on their cell phones than could ever fit in a wallet, address book, [or] briefcase." *United States v. Wurie*, 728 F.3d 1, 9 (1st Cir. 2013). Quantitatively, with their "immense storage capacity," electronic devices can contain "millions of pages of text, thousands of pictures, or hundreds of videos." *Riley*, 573 U.S. at 393-94. Qualitatively, electronic devices contain information "of a highly personal nature: photographs, videos, written and audio messages (text, email, and voicemail), contacts, calendar appointments, web search and browsing history, purchases, and financial and medical records." *Wurie*, 728 F.3d at 8.

Because these devices contain "the sum of an individual's private life," law enforcement in the interior of the United States typically must obtain a warrant before searching one. *Riley*, 573 U.S. at 394. However, both within the interior and at the border, the government regularly subjects the electronic devices of people on the Watchlist to warrantless searches.[14]

[14] Given the coercive, intrusive, and dangerous nature of a stop for a person on the Watchlist, *see* Part II.B.1., such an encounter may cause them to

Within the interior. The FBI expressly advises local police departments and other law enforcement agencies to collect more information when encountering an individual on the Watchlist than they would otherwise.[15] The FBI directs them to search any electronic device such an individual is carrying and to report their findings back to the federal government.[16] Moreover, the FBI advises law enforcement to create *copies* of data stored on or accessible from such devices, including social media accounts, address books, speed-dial numbers, photographs, medical information, and more.[17]

These efforts have been successful. Between 2015 and 2018, the federal government collected almost 5,000 new "biographical identifiers" through stops by local law enforcement, including license, passport, and

---

consent to a search of their electronic devices where they otherwise would not have.

[15] *See* FBI, *Watchlisting Guidance* 58-79 (Mar. 2013), https://assets.documentcloud.org/documents/1227228/2013-watchlist-guidance.pdf (describing "the types of information that a Department or Agency should consider collecting" during an encounter with someone on the Watchlist).

[16] *See id.* at 65-69 (listing over 120 discrete categories of information that law enforcement should try to search, including every type of electronic device).

[17] *See id.*

visa information, languages spoken, travel plans, and photographs and videos.[18]

At the border. An individual's inclusion on the Watchlist also increases the likelihood that they will face heightened screening at the border when they enter the United States, including extensive questioning, searches of their belongings and electronic devices, and detention. Many people on the Watchlist suffer searches and potential seizures of their electronic devices at the U.S. border. Indeed, in this case, eight plaintiffs have reported having their cell phones, laptops, or other devices searched, some even repeatedly. JA ___ [Dkt. 305 at 14-16]. Some reported that their traveling companions' devices were searched as well. *Id.* Some were pressured to hand over their passwords to enable more intrusive searches. *Id.*

Because of the extraordinary privacy interests at stake in electronic devices, increasingly, some courts recognize that border searches of electronic devices must be treated differently than searches of luggage or other belongings at the border. *See, e.g.*, *United States v. Cano*, 934 F.3d 1002, 1007 (9th Cir. 2019) (requiring that all electronic device searches at the border "be limited in scope to a search for digital contraband"); *Alasaad v. Nielsen*, 419 F. Supp. 3d 142, 165 (D. Mass. 2019) (holding that electronic device searches require border agents to have reasonable

[18] FBI, *US Law Enforcement Encounters*, *supra* note 13; de Bourmont & Winter, *supra* note 10 (quoting another FBI document).

suspicion that the device contains digital contraband), *appeal docketed*, Nos. 20-1077 & 20-1081 (1st Cir. Jan. 29, 2020). Indeed, this Court, too, has recognized that forensic border searches of electronic devices require, at minimum, reasonable suspicion. *See United States v. Aigbekaen*, 943 F.3d 713 (4th Cir. 2019); *United States v. Kolsuz*, 890 F.3d 133 (4th Cir. 2018).

Current U.S. Customs and Border Protection (CBP) policy allows for "basic" or "manual" searches, meaning scrolling or tapping through a device or using a built-in search function, without any suspicion of wrongdoing.[19] For "advanced" or "forensic" searches, where border agents attach external equipment to review or copy data, CBP policy ordinarily requires "reasonable suspicion of activity in violation of the laws enforced or administered by CBP."[20] But in the case of a national security concern, CBP policy permits a forensic search with no suspicion whatsoever.[21] In other words, even if there is no evidence of wrongdoing, being on the Watchlist means being subjected to the most intrusive types of device searches at the border.

The government claims that Watchlist status is "just one of many factors" that could lead to a search of an individual's electronic devices at the border. Opening Br. 37. In reality, however, being on the Watchlist

---

[19] *See* CBP Directive No. 3340-049A § 5.1.3 (Jan. 4, 2018).

[20] *Id.* § 5.1.4.

[21] *Id.*

drastically increases the chances that a person's devices will be searched when they appear at the border.

When deciding whether to search a traveler's device, CBP and U.S. Immigration and Customs Enforcement (ICE) officers consider information about the traveler that is stored in multiple government databases, including TECS, CBP's main database for border screening, and the Automated Targeting System (ATS). Pls.' Reply in Supp. of Pls.' Statement of Undisputed Material Facts ¶¶ 25, 35, 36, 38, 44, *Alasaad*, 419 F. Supp. 3d 142 (D. Mass. 2019), Dkt. 99-1 [hereinafter *Alasaad Undisputed Facts*]. TECS "accepts nearly all records from the [Watchlist]," and ATS compares information about travelers entering, transiting through, or exiting the country against law enforcement and intelligence databases, including the Watchlist.[22]

CBP and ICE, as well as other law enforcement agencies, can place "lookouts" in TECS that flag travelers for additional scrutiny during border crossings, which may include border searches of electronic devices. *Alasaad Undisputed Facts* ¶¶ 27-32. One reason a lookout may be created is a Watchlist match.[23] In addition, the information stored in border-screening databases may include the fact that border officers previously

---

[22] Bjelopera, *supra* note 2, at 8.

[23] U.S. Dep't of Homeland Security, *Privacy Impact Assessment for the TECS System: CBP Primary and Secondary Processing*, at 3 (Dec. 22, 2010), https://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_tecs.pdf.

searched the traveler's device or subjected them to other screening, a narrative description of the content observed during the previous search, and a copy of the data seized during a previous search. *Id.* ¶¶ 5, 26, 34, 37. This information about prior searches is another reason that a border-screening database may flag the traveler for heightened screening in the future. *Id.* ¶ 43.

The result is that being on the Watchlist creates a feedback loop: Watchlist status can serve as the impetus for a lookout that a CBP officer will see at primary inspection, after which the officer will send the traveler to secondary inspection. At secondary inspection, an officer may search the traveler's electronic devices and note in border-screening databases the fact of the search, a narrative description of the device's contents, and perhaps even a copy of the data on the device. And this screening and search, in turn, makes it more likely that the traveler will be stopped at the border and their devices will be searched in the future.

Rather than try to mitigate this potential for circular reasoning and escalation, the government actively fuels this feedback loop:[24] a border agent can search through an individual's electronic devices, and even seize

[24] *See* CBP Directive, *supra* note 19, at § 5.1.3 (no suspicion required for manual searches) & § 5.1.4 (for forensic searches, "[m]any factors may create reasonable suspicion or constitute a national security concern; examples include . . . the presence of an individual on a government-operated and government-vetted terrorist watchlist").

a copy of the data, exposing the individual's "privacies of life" every time they come to the border based solely on their inclusion on the Watchlist.

3. Immigration benefits become practically impossible to obtain

In addition to the many law-enforcement-related harms a listee may face due to inclusion on and dissemination of the Watchlist, they can also face harms in other parts of their life. U.S. Citizenship and Immigration Services (USCIS) has an express, yet secret, policy of delaying and denying applications for immigration benefits from those on the Watchlist that is currently the subject of active litigation. *Wagafe v. U.S. Citizenship & Immigration Servs.*, No. 2:17-cv-00094-RAJ (W.D. Wash. filed Jan. 23, 2017). Formally, the Controlled Application Review and Resolution Program (CARRP) is USCIS's policy for "identifying and processing cases with national security (NS) concerns" and applies to "all applications and petitions that convey immigrant or nonimmigrant status."[25] CARRP is designed to "ensure that immigration benefits are not granted to individuals and organizations that pose a threat to national security."[26]

---

[25] Jonathan R. Scharfen, *Policy for Vetting and Adjudicating Cases with National Security Concerns*, USCIS 1 & n.4 (Apr. 11, 2008), https://www.uscis.gov/sites/default/files/USCIS/About%20Us/Electronic%20Reading%20Room/Policies_and_Manuals/CARRP_Guidance.pdf.

[26] U.S. Citizenship & Immigration Servs., *CARRP Officer Training: National Security Handouts* 2 (Apr. 2009), *available at* https://www.aclusocal.org/sites/default/files/wp-content/uploads/2013/01/Guiance-for-Identifying-NS-Concerns-USCIS-CARRP-Training-Mar.-2009.pdf.

CARRP defines a national security concern as

> an individual or organization [that] has been determined to have an articulable link to prior, current, or planned involvement in, or association with, an activity, individual or organization described in [the security and terrorism sections] of the Immigration and Nationality Act.[27]

This is similar to the reasonable suspicion standard for placing someone on the Watchlist.[28] Despite this vague standard, CARRP provides that anyone on the Watchlist is automatically subject to CARRP procedures.[29]

CARRP instructs USCIS officers to scrutinize applicants on the Watchlist for *any* basis to deny the application—beyond what they would for a routine adjudication. CARRP demands that USCIS officers search applications for anything from false testimony to minor oversights or inconsistencies that might be used as a pretext for denial.[30] For example,

---

[27] Scharfen, *supra* note 25, at 1 n.1.

[28] *See* Bjelopera, *supra* note 2, at 4. Notably, this definition does not actually require an individual to be suspected of engaging in unlawful activity or of joining a designated terrorist organization to be deemed a national security concern; merely traveling to or residing in areas of terrorist activity, or associating with individuals suspected of engaging in suspicious activities, is sufficient. *See* Amended Complaint ¶¶ 73-87, *Wagafe*, No. 2:17-cv-00094-RAJ.

[29] Bjelopera, *supra* note 2, at 9; *CARRP Officer Training*, *supra* note 26, at 2.

[30] *See* USCIS, *Controlled Application Review and Resolution Program (CARRP)* 52-58 (Jan. 2012), *available at* Ex. C to Decl. of Jennie Pasquarella, *Wagafe*, No. 2:17-cv-00094-RAJ (W.D. Wash. Feb. 9, 2017), Dkt. 27-1 at 58-65, 74.

some possibilities CARRP suggests are omission of a prior address or failure to disclose a charitable contribution, as well as retrospective ineligibility for any previously granted immigration benefit.[31] Even without a pretextual basis to *deny* an application, USCIS officers cannot *approve* applications from individuals on the Watchlist.[32] Instead, CARRP instructs officers to send the application to USCIS headquarters for an ultimate decision.[33] Headquarters, in turn, will not approve such an application unless the Deputy Director of the USCIS permits it.[34]

If being on the Watchlist merely influenced USCIS's determination, that would be enough to alter a person's legal status for purposes of the stigma-plus standard. *See Humphries*, 554 F.3d at 1187-88. Here, the impact is even greater. For everything from supposedly nondiscretionary naturalization applications to more discretionary immigration benefits, the presumption becomes denial. That is more than enough alteration in status to establish the "plus" element. *See Cannon*, 891 F.3d at 502-03; *Humphries*, 554 F.3d at 1187-88.

4. Economic opportunities are denied

Individuals on the Watchlist often lose out on economic opportunities. They are fired from or denied jobs that require travel. First

---

[31] *See id*.

[32] Scharfen, *supra* note 25, at 7.

[33] *Id.*

[34] *Id.* at 27.

Amended Complaint ¶¶ 401-07, *El Ali v. Barr*, No. 8:18-cv-02415-PX (D. Md.), Dkt. 48 [hereinafter *El Ali Complaint*]. They lose jobs and contracts that require them to enter military bases. *Id.* ¶¶ 704, 950-53; *see* JA ___ [Plaintiffs' MSJ Ex. 62 at 5, Ex. 57] (people on the Watchlist are barred from entering military bases). They are denied Customs seals and Transportation Worker Identification Credentials, and lose jobs for that reason as well. JA __ [Dkt. 305-9 at 20-21]; *El Ali Complaint* ¶¶ 1043-46. Some have been denied access to banks and credit. *See, e.g.*, *Kovac v. Wray*, 363 F. Supp. 3d 721, 736 (N.D. Tex. 2019); *El Ali Complaint* ¶¶ 881, 1008-09, 1205-06, 1350.

5. Watchlist information is at risk of misuse or breach

Finally, the secrecy with which the government treats the Watchlist makes it impossible to determine whether it has been misused. But government agencies' documented pattern of database misuse, coupled with the salacious nature of the allegation associated with being on the Watchlist, raises serious concerns about whether the Watchlist has been, or could be, at risk of misuse or breach.

Government agencies previously have been found to misuse sensitive databases. For example, an internal audit of the National Security Agency revealed the "unauthorized use of data about more than 3,000 Americans and green-card holders."[35] The pattern holds at the local level,

[35] Barton Gellman, *NSA broke privacy rules thousands of times per year, audit finds*, Wash. Post (Aug. 15, 2013),

too. A 2016 Associated Press investigation based on public records requests found that the very databases that give officers critical information about people they encounter can also be misused for purposes such as "voyeuristic curiosity"; in egregious cases, officers have "used information to stalk or harass, or have tampered with or sold records they obtained."[36] In at least one instance, police officers maliciously added an innocent man to a state-level gang member watchlist analogous to the federal government's Watchlist at issue in this case.[37]

Personal information can also be at risk of breach because of the Watchlist's wide dissemination. Just last year, CBP suffered a data breach that compromised photos and license plates for nearly 100,000 travelers at a single port of entry at the U.S.-Canada border.[38] CBP blamed a subcontractor's violation of "mandatory security and privacy protocols" as

---

https://www.washingtonpost.com/world/national-security/nsa-broke-privacy-rules-thousands-of-times-per-year-audit-finds/2013/08/15/3310e554-05ca-11e3-a07f-49ddc7417125_story.html.

[36] Sadie Gurman, *Across US, police officers abuse confidential databases*, Assoc. Press (Sept. 28, 2016), https://apnews.com/699236946e3140659fff8a2362e16f43.

[37] Tonya Mosley, *LAPD Under Review By California AG For Alleged Misuse Of The State's Gang Database*, WBUR (Feb. 17, 2020), https://www.wbur.org/hereandnow/2020/02/17/lapd-calgang-california-misuse.

[38] Kate Sullivan & Geneva Sands, *Feds say photos of travelers compromised in data breach*, CNN (June 10, 2019), https://www.cnn.com/2019/06/10/politics/customs-and-border-protection-images-travelers-data-breach/index.html.

one of the causes of the breach.[39] There is no reason, and the government has provided none, to believe that the Watchlist is any more secure.

* * *

This brief is far from a complete list of the harms people suffer from being put on the Watchlist. The point is this: being on the Watchlist alters and extinguishes a wide variety of rights and legal statuses—with virtually no process. The Due Process Clause forbids that.

CONCLUSION

For all these reasons, the Court should hold that Plaintiffs have satisfied the elements of a stigma-plus claim.

Dated: June 2, 2020

Respectfully submitted,

By: */s/Athul K. Acharya*
Matthew Borden
Athul K. Acharya
Gunnar Martz

BRAUNHAGEY & BORDEN LLP

/s/Saira Hussain
Saira Hussain
Mark Rumold
Kit Walsh

ELECTRONIC FRONTIER FOUNDATION

Counsel for *Amicus Curiae*

[39] *Id.*

UNITED STATES COURT OF APPEALS FOR THE FOURTH CIRCUIT

DISCLOSURE STATEMENT

- In civil, agency, bankruptcy, and mandamus cases, a disclosure statement must be filed by **all** parties, with the following exceptions: (1) the United States is not required to file a disclosure statement; (2) an indigent party is not required to file a disclosure statement; and (3) a state or local government is not required to file a disclosure statement in pro se cases. (All parties to the action in the district court are considered parties to a mandamus case.)
- In criminal and post-conviction cases, a corporate defendant must file a disclosure statement.
- In criminal cases, the United States must file a disclosure statement if there was an organizational victim of the alleged criminal activity. (See question 7.)
- Any corporate amicus curiae must file a disclosure statement.
- Counsel has a continuing duty to update the disclosure statement.

No. 20-1119 Caption: Elhady v. Kable

Pursuant to FRAP 26.1 and Local Rule 26.1,

Electronic Frontier Foundation
(name of party/amicus)

who is amicus curiae, makes the following disclosure:
(appellant/appellee/petitioner/respondent/amicus/intervenor)

1. Is party/amicus a publicly held corporation or other publicly held entity? ☐YES ☑NO

2. Does party/amicus have any parent corporations? ☐YES ☑NO
If yes, identify all parent corporations, including all generations of parent corporations:

3. Is 10% or more of the stock of a party/amicus owned by a publicly held corporation or other publicly held entity? ☐YES ☑NO
If yes, identify all such owners:

4. Is there any other publicly held corporation or other publicly held entity that has a direct financial interest in the outcome of the litigation? ☐YES ☑NO
If yes, identify entity and nature of interest:

5. Is party a trade association? (amici curiae do not complete this question) ☐YES ☐NO
If yes, identify any publicly held member whose stock or equity value could be affected substantially by the outcome of the proceeding or whose claims the trade association is pursuing in a representative capacity, or state that there is no such member:

6. Does this case arise out of a bankruptcy proceeding? ☐YES ☑NO
If yes, the debtor, the trustee, or the appellant (if neither the debtor nor the trustee is a party) must list (1) the members of any creditors' committee, (2) each debtor (if not in the caption), and (3) if a debtor is a corporation, the parent corporation and any publicly held corporation that owns 10% or more of the stock of the debtor.

7. Is this a criminal case in which there was an organizational victim? ☐YES ☑NO
If yes, the United States, absent good cause shown, must list (1) each organizational victim of the criminal activity and (2) if an organizational victim is a corporation, the parent corporation and any publicly held corporation that owns 10% or more of the stock of victim, to the extent that information can be obtained through due diligence.

Signature: /s/Saira Hussain Date: June 2, 2020

Counsel for: Electronic Frontier Foundation

Print to PDF for Filing

UNITED STATES COURT OF APPEALS FOR THE FOURTH CIRCUIT
Effective 12/01/2016

No. 20-1119 **Caption:** Elhady v. Kable

CERTIFICATE OF COMPLIANCE WITH TYPE-VOLUME LIMIT

Type-Volume Limit, Typeface Requirements, and Type-Style Requirements

Type-Volume Limit for Briefs: Appellant's Opening Brief, Appellee's Response Brief, and Appellant's Response/Reply Brief may not exceed 13,000 words or 1,300 lines. Appellee's Opening/Response Brief may not exceed 15,300 words or 1,500 lines. A Reply or Amicus Brief may not exceed 6,500 words or 650 lines. Amicus Brief in support of an Opening/Response Brief may not exceed 7,650 words. Amicus Brief filed during consideration of petition for rehearing may not exceed 2,600 words. Counsel may rely on the word or line count of the word processing program used to prepare the document. The word-processing program must be set to include headings, footnotes, and quotes in the count. Line count is used only with monospaced type. See Fed. R. App. P. 28.1(e), 29(a)(5), 32(a)(7)(B) & 32(f).

Type-Volume Limit for Other Documents if Produced Using a Computer: Petition for permission to appeal and a motion or response thereto may not exceed 5,200 words. Reply to a motion may not exceed 2,600 words. Petition for writ of mandamus or prohibition or other extraordinary writ may not exceed 7,800 words. Petition for rehearing or rehearing en banc may not exceed 3,900 words. Fed. R. App. P. 5(c)(1), 21(d), 27(d)(2), 35(b)(2) & 40(b)(1).

Typeface and Type Style Requirements: A proportionally spaced typeface (such as Times New Roman) must include serifs and must be 14-point or larger. A monospaced typeface (such as Courier New) must be 12-point or larger (at least 10½ characters per inch). Fed. R. App. P. 32(a)(5), 32(a)(6).

This brief or other document complies with type-volume limits because, excluding the parts of the document exempted by Fed. R. App. R. 32(f) (cover page, disclosure statement, table of contents, table of citations, statement regarding oral argument, signature block, certificates of counsel, addendum, attachments):

☑ this brief or other document contains 6,004 [*state number of*] words

☐ this brief uses monospaced type and contains _____ [*state number of*] lines

This brief or other document complies with the typeface and type style requirements because:

☑ this brief or other document has been prepared in a proportionally spaced typeface using
Microsoft Word [*identify word processing program*] in
14-pt, Times New Roman [*identify font size and type style*]; **or**

☐ this brief or other document has been prepared in a monospaced typeface using
_____ [*identify word processing program*] in
_____ [*identify font size and type style*].

(s) /s/ Athul K. Acharya

Party Name Electronic Frontier Foundation

Dated: June 2, 2020

UNITED STATES COURT OF APPEALS FOR THE FOURTH CIRCUIT

APPEARANCE OF COUNSEL FORM

BAR ADMISSION & ECF REGISTRATION: If you have not been admitted to practice before the Fourth Circuit, you must complete and return an Application for Admission before filing this form. If you were admitted to practice under a different name than you are now using, you must include your former name when completing this form so that we can locate you on the attorney roll. Electronic filing by counsel is required in all Fourth Circuit cases. If you have not registered as a Fourth Circuit ECF Filer, please complete the required steps at Register for eFiling.

THE CLERK WILL ENTER MY APPEARANCE IN APPEAL NO. 20-1119, 20-1311 as

☐ Retained ☐ Court-appointed(CJA) ☐ CJA associate ☐ Court-assigned(non-CJA) ☐ Federal Defender

☑ Pro Bono ☐ Government

COUNSEL FOR: Electronic Frontier Foundation

_____ as the
(party name)

☐ appellant(s) ☐ appellee(s) ☐ petitioner(s) ☐ respondent(s) ☑ amicus curiae ☐ intervenor(s) ☐ movant(s)

/s/ Athul K. Acharya
(signature)

Please compare your information below with your information on PACER. Any updates or changes must be made through PACER's Manage My Account.

Athul K. Acharya Name (printed or typed)	(415) 599-0210 Voice Phone
BraunHagey & Borden LLP Firm Name (if applicable)	(415) 276-1808 Fax Number
351 California St, 10th Floor San Francisco, CA 94104 Address	acharya@braunhagey.com E-mail address (print or type)

CERTIFICATE OF SERVICE *(required for parties served outside CM/ECF)*: I certify that this document was served on _____ by ☐ personal delivery; ☐ mail; ☐ third-party commercial carrier; or ☐ email (with written consent) on the following persons at the addresses or email addresses shown:

_____ _____
Signature Date

1/28/2020 SCC