# Resolved: The NSA should end its surveillance of U.S. citizens and lawful permanent residents.

## Pro

#### Framing:

Cost-Benefit Analysis; weigh impacts based on their net implications

### Contention: Personal Rights

#### UQ: NSA conducts overbearing, unjust surveillance

Bamford 15

James Bamford writes for Reuters, Why NSA surveillance is worse than you’ve ever imagined, Published by Reuters 5/11/15, http://blogs.reuters.com/great-debate/2015/05/11/if-youre-not-outraged-about-the-nsa-surveillance-heres-why-you-should-be/)//LED

Last summer, after months of encrypted emails, I spent three days in Moscow hanging out with Edward Snowden for a Wired cover story. Over pepperoni pizza, he told me that what finally drove him to leave his country and become a whistleblower was his conviction that the National Security Agency was conducting illegal surveillance on every American. Thursday, the Second Circuit Court of Appeals in New York agreed with him. In a long-awaited opinion, the three-judge panel ruled that the NSA program that secretly intercepts the telephone metadata of every American — who calls whom and when — was illegal. As a plaintiff with Christopher Hitchens and several others in the original ACLU lawsuit against the NSA, dismissed by another appeals court on a technicality, I had a great deal of personal satisfaction. It’s now up to Congress to vote on whether or not to modify the law and continue the program, or let it die once and for all. Lawmakers must vote on this matter by June 1, when they need to reauthorize the Patriot Act. Edward\_Snowden-wiki Edward Snowden during an interview with Glenn Greenwald and Laura Poitras, June 6, 2013. WIKIPEDIA/Screenshot of a Laura Poitras film by Praxis Films A key factor in that decision is the American public’s attitude toward surveillance. Snowden’s revelations have clearly made a change in that attitude. In a PEW 2006 survey, for example, after the New York Times’ James Risen and Eric Lichtblau revealed the agency’s warrantless eavesdropping activities, 51 percent of the public still viewed the NSA’s surveillance programs as acceptable, while 47 percent found them unacceptable. After Snowden’s revelations, those numbers reversed. A PEW survey in March revealed that 52 percent of the public is now concerned about government surveillance, while 46 percent is not. Given the vast amount of revelations about NSA abuses, it is somewhat surprising that just slightly more than a majority of Americans seem concerned about government surveillance. Which leads to the question of why? Is there any kind of revelation that might push the poll numbers heavily against the NSA’s spying programs? Has security fully trumped privacy as far as the American public is concerned? Or is there some program that would spark genuine public outrage? Few people, for example, are aware that a NSA program known as TREASUREMAP is being developed to continuously map every Internet connection — cellphones, laptops, tablets — of everyone on the planet, including Americans. “Map the entire Internet,” says the top secret NSA slide. “Any device, anywhere, all the time.” It adds that the program will allow “Computer Attack/Exploit Planning” as well as “Network Reconnaissance.” One reason for the public’s lukewarm concern is what might be called NSA fatigue. There is now a sort of acceptance of highly intrusive surveillance as the new normal, the result of a bombardment of news stories on the topic. I asked Snowden about this. “It does become the problem of one death is a tragedy and a million is a statistic,” he replied, “where today we have the violation of one person’s rights is a tragedy and the violation of a million is a statistic. The NSA is violating the rights of every American citizen every day on a comprehensive and ongoing basis. And that can numb us. That can leave us feeling disempowered, disenfranchised.” An illustration picture shows logos of Google and Yahoo connected with LAN cables in Berlin An illustration picture shows the logos of Google and Yahoo connected with LAN cables in a Berlin office, October 31, 2013. REUTERS/Pawel Kopczynski​ In the same way, at the start of a war, the numbers of Americans killed are front-page stories, no matter how small. But two years into the conflict, the numbers, even if far greater, are usually buried deep inside a paper or far down a news site’s home page. In addition, stories about NSA surveillance face the added burden of being technically complex, involving eye-glazing descriptions of sophisticated interception techniques and analytical capabilities. Though they may affect virtually every American, such as the telephone metadata program, because of the enormous secrecy involved, it is difficult to identify specific victims. The way the surveillance story appeared also decreased its potential impact. Those given custody of the documents decided to spread the wealth for a more democratic assessment of the revelations. They distributed them through a wide variety of media — from start-up Web publications to leading foreign newspapers. One document from the NSA director, for example, indicates that the agency was spying on visits to porn sites by people, making no distinction between foreigners and “U.S. persons,” U.S. citizens or permanent residents. He then recommended using that information to secretly discredit them, whom he labeled as “radicalizers.” But because this was revealed by The Huffington Post, an online publication viewed as progressive, and was never reported by mainstream papers such as the New York Times or the Washington Post, the revelation never received the attention it deserved. Another major revelation, a top-secret NSA map showing that the agency had planted malware — computer viruses — in more than 50,000 locations around the world, including many friendly countries such as Brazil, was reported in a relatively small Dutch newspaper, NRC Handelsblad, and likely never seen by much of the American public. A parabolic reflector with a diameter of 18.3 metres (60 ft.) is pictured at the former monitoring base of the National Security Agency (NSA) in Bad Aibling ​A parabolic reflector with a diameter of 18.3 metres (60 ft.) at the National Security Agency’s former monitoring base in Bad Aibling, south of Munich, June 6, 2014. REUTERS/Michaela Rehle Thus, despite the volume of revelations, much of the public remains largely unaware of the true extent of the NSA’s vast, highly aggressive and legally questionable surveillance activities. With only a slim majority of Americans expressing concern, the chances of truly reforming the system become greatly decreased. While the metadata program has become widely known because of the numerous court cases and litigation surrounding it, there are other NSA surveillance programs that may have far greater impact on Americans, but have attracted far less public attention. In my interview with Snowden, for example, he said one of his most shocking discoveries was the NSA’s policy of secretly and routinely passing to Israel’s Unit 8200 — that country’s NSA — and possibly other countries not just metadata but the actual contents of emails involving Americans. This even included the names of U.S. citizens, some of whom were likely Palestinian-Americans communicating with relatives in Israel and Palestine. An illustration of the dangers posed by such an operation comes from the sudden resignation last year of 43 veterans of Unit 8200, many of whom are still serving in the military reserves. The veterans accused the organization of using intercepted communication against innocent Palestinians for “political persecution.” This included information gathered from the emails about Palestinians’ sexual orientations, infidelities, money problems, family medical conditions and other private matters to coerce people into becoming collaborators or to create divisions in their society. Another issue few Americans are aware of is the NSA’s secret email metadata collection program that took place for a decade or so until it ended several years ago. Every time an American sent or received an email, a record was secretly kept by the NSA, just as the agency continues to do with the telephone metadata program. Though the email program ended, all that private information is still stored at the NSA, with no end in sight. With NSA fatigue setting in, and the American public unaware of many of the agency’s long list of abuses, it is little wonder that only slightly more than half the public is concerned about losing their privacy. For that reason, I agree with Frederick A. O. Schwartz Jr., the former chief counsel of the Church Committee, which conducted a yearlong probe into intelligence abuses in the mid-1970s, that we need a similarly thorough, hard-hitting investigation today. “Now it is time for a new committee to examine our secret government closely again,” he wrote in a recent Nation magazine article, “particularly for its actions in the post-9/11 period.” Until the public fully grasps and understands how far over the line the NSA has gone in the past — legally, morally and ethically — there should be no renewal or continuation of NSA’s telephone metadata program in the future.

#### Surveillance is not all created equally-we must recognize the power distribution

Barton and Adler-Bell 17

Barton Gellman is an author, journalist and senior fellow at the Century Foundation, Sam Adler-Bell is a Century Foundation Contributor, The Disparate Impact of Surveillance, Published 12/21/17 by Century Foundation, <https://tcf.org/content/report/disparate-impact-surveillance/?session=1)//LED>

Mass surveillance society subjects us all to its gaze, but not equally so. Its power touches everyone, but its hand is heaviest in communities already disadvantaged by their poverty, race, religion, ethnicity, and immigration status. Technology and stealth allow government watchers to remain unobtrusive when they wish to be so, but their blunter tools—stop-and-frisk,1 suspicionless search, recruitment of snitches, compulsory questioning on intimate subjects—are conspicuous in the lives of those least empowered to object. We are not exactly the first to notice2 these disparities. There is a rich and diverse literature of dissent, hard experience, and scholarship about the disproportionate intrusions of government into poor and brown communities, much of it produced by people with roots in those precincts themselves. We are indebted to their work. We will make no pretense here of explaining the unjust burdens of surveillance to people who have carried and protested them for decades. We direct our report, instead, to people who could have listened but did not: lawmakers, law enforcement authorities, mayors, governors, and other people with power who failed to look beyond their own experience and point of view. Most of all, we aim this report at our fellow thinkers about surveillance on a national and global scale. For decades, and especially in the past four years, civil libertarians (including the authors of this report) have tended to frame this debate in the discourse of universal rights.3 We assert a place for privacy among the core liberties that restrain state power in a self-governing democracy. Through that lens, government surveillance is seen as inflicting its harms on everyone. Even when ostensibly targeted, its methods tend to encroach on the public at large. All of us, consciously or not, have something to hide—something that would harm us or people we know if revealed in the wrong circumstance.4 We stand by these positions. We have also come to see them as profoundly incomplete. Universalist arguments obscure the topography of power. Surveillance is not at all the same thing at higher and lower elevations on the contour map of privilege. Privacy scholars speak of philosophical rights and hypothetical risks; privacy-minded middle class Americans fear allowing the government too much access to their electronic trails. But there is nothing abstract about the physical, often menacing, intrusions into less fortunate neighborhoods, where mere presence in a “high-crime” area is grounds for detention, search, and questioning by police. At age sixty-five, tens of millions of Americans5 claim their Medicare benefits with nothing more eventful than completion of some forms. (Medicare.gov even promises to “protect your privacy by getting rid of the information you give us when you close the browser.”)6 An impoverished single mother on Medicaid faces mortifying questions, face-to-face with benefit managers, about her lovers, hygiene, parental shortcomings, and personal habits.7

#### These disparities hold inherent impacts, and must frame how we view this debate. Reductions necessary

Barton and Adler-Bell 17

Barton Gellman is an author, journalist and senior fellow at the Century Foundation, Sam Adler-Bell is a Century Foundation Contributor, The Disparate Impact of Surveillance, Published 12/21/17 by Century Foundation, <https://tcf.org/content/report/disparate-impact-surveillance/?session=1)//LED>

This report gives primary attention to the disparate impact of surveillance made manifest through urban policing and social services for the poor. Not everyone is accustomed to viewing these systems through the lens of surveillance, but a substantial body of research has done so for years. In the lived experience of minority neighborhoods, authorities at ground level wield enormous power to peer into their lives. Privacy is not only a luxury that many residents cannot afford. In surveillance-heavy precincts, for practical purposes, privacy cannot be bought at any price. Unspoken policy, well intended or not, disqualifies those people from basic protections8 that most Americans can take for granted. Privacy advocates have sometimes struggled to demonstrate the harms of government surveillance to the general public. Part of the challenge is empirical. Federal, state, and local governments shield their high-technology operations with stealth, obfuscation, and sometimes outright lies when obliged to answer questions. In many cases, perhaps most, these defenses defeat attempts to extract a full, concrete accounting of what the government knows about us, and how it puts that information to use. There is a lot less mystery for the poor and disfavored, for whom surveillance takes palpable, often frightening forms. Universalist arguments apply across lines of social and economic class, but their generality is not well suited to combating unequal and particular harms. Members of our most disadvantaged communities have long asserted that they fall under heavier and more hostile scrutiny, and empirical research supports them. Meaningful oversight of state surveillance cannot be designed with only common conditions in mind. There is no sense in having a conversation about surveillance in America without taking account of its profoundly unequal use. We cannot divorce privacy research or policy from considerations of class, race, gender, and other social hierarchies. When we do that, as we do often, we fail. The liberal conception of privacy has no claim to universal reach if it fails to adapt to unequal circumstance. The Birth of “Privacy” The concept of privacy was conceived in counterpoint to the government’s growing ambition to peer inside long-closed compartments of our personal lives. The struggle took place most often in court. The leading cases mark milestones in that history, and show the disproportionate place of minority surveillance in the evolution of law. The provenance of privacy as a legal right is generally traced to Louis D. Brandeis. In “The Right to Privacy,” published in the Harvard Law Review9 in 1890, Brandeis and Samuel D. Warren, his law partner and former classmate, made the case for a “right to be let alone”10 embedded in English Common Law.11 Seventy-five years passed before the Supreme Court gave its blessing to a version of that claim. In 1928, by then an associate justice of the U.S. Supreme Court, Brandeis wrote an influential dissent in Olmstead v. United States that reframed the right to privacy in constitutional, not Common Law, terms. The majority in Olmstead upheld a warrantless wiretap because police had not trespassed on the defendant’s property or searched his “tangible material effects.” In his dissent, Brandeis wrote that “material things” and places were not the main concern of the Founders. “They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations,” he wrote. “They conferred, as against the government, the right to be let alone—the most comprehensive of rights and the right most valued by civilized men.”12 An “unjustifiable intrusion,” whether or not by physical trespass, breached the Fourth Amendment.13 The use of evidence so obtained in a criminal case, he wrote, “must be deemed a violation of the Fifth.”14

#### Discrepancies exist and must be eliminated all together

Barton and Adler-Bell 17

Barton Gellman is an author, journalist and senior fellow at the Century Foundation, Sam Adler-Bell is a Century Foundation Contributor, The Disparate Impact of Surveillance, Published 12/21/17 by Century Foundation, <https://tcf.org/content/report/disparate-impact-surveillance/?session=1)//LED>

In obvious and less obvious ways, wealth plays a role in defining who and what the Fourth Amendment protects. Apart from the Brandeis dissent noted earlier, the Olmstead case was an unexceptional affirmation of precedent. Chief Justice William H. Taft wrote for the majority that the Fourth Amendment had no bearing on searches of places and things outside a defendant’s home or property. The government required no warrant to eavesdrop on calls made by Roy Olmstead, an ex-cop turned bootlegger, because the telephone wires “are not part of his house or office, any more than are the highways along which they are stretched.”32 Decades later, in another wiretap case, the U.S. Supreme Court shifted course. In Katz v. United States, decided in 1967, the Court embraced Brandeis’s argument that a search need not involve physical trespass to cross a constitutional line. Authorities had eavesdropped on the defendant at a telephone booth, not on his property, but the court ruled he had a “reasonable expectation of privacy” nonetheless. Justice John Marshall Harlan addressed the obvious ambiguity of that phrase in a concurring opinion. Harlan proposed two tests: “[F]irst that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as ‘reasonable.’”33 Katz did not stray as far from Olmstead as first appeared. Privacy and property were still entwined, if less directly, by the nature of the factual question that Harlan asked. Could a reasonable person in the defendant’s shoes expect to stay out of earshot at the time and place of the wiretap? If so, surveillance without a warrant was analogous to peering inside a private home. Katz made his case successfully because he placed his illegal gambling calls in a telephone booth with a door that closed and glass walls that allowed him to keep an eye on surroundings. If a nearby stranger could have listened in,34 on the other hand, police could do the same on their own authority. The Katz doctrine in practice came to mean that “privacy follows space,” not citizens, as late legal scholar William Stuntz observed.35 Unobserved space costs money. A class-statified spectrum of legal privilege took shape in the cases that followed Katz. Trial and appellate courts found, not unreasonably, that citizens had the strongest expectations of privacy in their homes, somewhat less in their cars, and not much at all on public streets or public transport, however intimate the words they exchanged with a seatmate on the bus.36 A nosy passenger behind them might overhear, and government authorities therefore felt free, without contradiction yet from the courts, to place hidden microphones under the seats.37 Class-inflected hierarchies did not stop there. White-collar workers with office doors had legal rights against warrantless surveillance that did not apply on the shop floor38 or a construction site. Property ownership did not formally define a person’s Fourth Amendment rights, but a fenced-in yard,39 a house set back from the street, a bit of “curtilage”40 at the property line, or even curtained windows might decide whether Fourth Amendment protections applied. Thin-walled apartments in densely packed towers made for porous shields at best. The poor have little choice but to live out their private lives in public spaces: parks and courtyards, empty lots, sidewalk stoops. The homeless, with still fewer sanctuaries, have correspondingly even weaker legal claims to a “reasonable expectation of privacy.”41 Together, these precedents have created an unequal distribution of privacy rights. The richer you are, the more privacy you enjoy; the poorer, the less. In 2012, the Court adjusted course again. By unanimous vote it reversed a verdict against an alleged drug dealer convicted with tracking data from a GPS device that police placed surreptitiously on his car. The Justice Department, following precedent, maintained that anyone might have seen the defendant as he drove public streets and thus the FBI was free to track him too. In United States v. Jones, the Supreme Court disagreed, ruling that electronic surveillance of this sort counted as a “search” under the Fourth Amendment and therefore required a warrant based upon probable cause. The Justices disagreed, however, on why. The only argument that carried a majority was that, as Justice Antonin Scalia put it, police had failed “the common law trespassory test”42 by sneaking onto the defendant’s driveway for access to his car. In that respect, despite hints of a broader doctrine to come, Jones reinforced the old property-bound conception of privacy. Carpenter v. United States,43 which went to oral argument on November 29 of this year, presents a similar set of facts without a trespass on private property. (Police tracked the defendant by his mobile phone’s contact with cell towers.) The court’s decision, now pending, has the potential to set a new doctrine for the Fourth Amendment in the electronic age.

#### Radical reform is required-we must eliminate

Barton and Adler-Bell 17

Barton Gellman is an author, journalist and senior fellow at the Century Foundation, Sam Adler-Bell is a Century Foundation Contributor, The Disparate Impact of Surveillance, Published 12/21/17 by Century Foundation, <https://tcf.org/content/report/disparate-impact-surveillance/?session=1)//LED>

Laws and norms that safeguard privacy in the United States do not work for poor people, racial minorities, or otherwise disfavored groups. As practiced in contemporary America, surveillance leaves them open to arbitrary and encompassing intrusions that are seldom if ever inflicted upon society at large. Why this is the case—the question of intent—is beyond the scope of this report. The systems we have examined—public safety and social welfare—are created and supported by many well-intentioned people in good faith. They need not be malicious by design, however, to have harmful effects. Cybernetic theorist Stafford Beer’s maxim that “the purpose of a system is what it does” is instructive in this regard. It’s not sufficient to dismiss the significant harms of our policing and welfare systems as unfortunate side-effects. For one thing, a model that blames every harm on righteous accident cannot plausibly cover all the abuses we have documented here. Some of of the harshest surveillance measures are features, not bugs, in the system. Discriminatory surveillance and control are not epiphenomenal to the project of providing for the poor; they are purposeful aspects of its design. And their persistence is a political choice. Addressing the disparate harms of surveillance means developing a more capacious concept of “privacy” that is attentive to the experience of those who live beyond its practical reach. Some of our finest thinkers on surveillance have cabined themselves off from facts on the ground in unfamiliar neighborhoods. Some of our finest thinkers on surveillance have cabined themselves off from facts on the ground in unfamiliar neighborhoods. Inattention to the experiences of non-white, non-male, and non-rich people produces embarrassing results, even in otherwise rigorous work.118 In a critique of Daniel Solove’s influential Taxonomy of Privacy, for example, Ann Bartow faults him for reducing the harms of surveillance to a feeling of “discomfort” and “unease.”119 A similar failure of imagination is suggested by James P. Nehf’s assertions that “privacy is seldom a matter of life and death” and that “most of the injuries caused by the misuse of data in modern society are not particularly embarrassing or emotionally disturbing.”120 As we have tried to demonstrate, arbitrary government intrusions in the terrains of East New York or Chicago’s West Side are routinely accompanied by humiliation, physical force, the risk of a lethal encounter, or crushing financial pressure. Traditional thinking about privacy rights has not addressed the practical limits of its reach. The trouble with the right to privacy as the catchall concept is that it imagines the bearer of such a right “as a self-determining, unencumbered individual, a being connected to others only by choice.”121 The gentleman in that picture bears no resemblance to the more typical targets of police and welfare surveillance that we have encountered in these pages. The presumption of self-sufficiency in the asserted right “to be let alone” is not germane to men and women whose lives are defined by poverty and interdependence.122 “Man’s Castle,” without a castle, is no shelter. When privacy is conceived as an abstract, egocentric right, it becomes difficult to defend against invocations of necessity to protect important interests of society at large. As Gilliom notes, “new surveillance initiatives are almost always in pursuit of broad social goods like reducing crime, drug use, or welfare fraud,” against which “the lonely and selfish claim to privacy just can’t stand up.” Those interests are overused to justify surveillance, but they are real. Likewise, the ostensible tradeoffs of privacy and security are frequently misconceived. Not for nothing does the Fourth Amendment begin with the words, “The right of the people to be secure….” Deprivations of privacy and security tend to walk in lockstep among poor and marginalized populations under surveillance. As we have seen, policing can instill terror; surveillance can ruin lives. When we speak of privacy and security, we would do well to ask: privacy for whom, and security against whom? These are questions and problems that the judicial branch is unsuited to resolve. The U.S. Supreme Court’s forthcoming decision in Carpenter may or may not mark a break from decades of sterile Fourth Amendment analysis, much of it based on risible presumptions of fact about the privacy we expect and the privacy we “voluntarily” choose to waive. In broader perspective, the Court will not and arguably should not become the engine of fundamental reform in this space. Within any foreseeable future, the Court’s majority will not discover a constitutional right to privacy that is robust enough to address the abuses we have described here. Some legal scholars hold out hope for progress by way of a doctrine against what are known as “unconstitutional conditions.”123 The doctrine states, in short, that government may not require anyone to cede a constitutional right in exchange for a public benefit.124 That might be a powerful weapon of reform if the Court were not committed to sidestepping its implications. As we have seen, the Court distinguishes fundamentally between “direct state interference with a protected activity” and a “mere refusal to subsidize a protected activity” (emphasis added). The Court acknowledged in Goldberg v. Kelly (1970) that “forces not within the control of the poor contribute to their poverty.”125 It accepted in Harris v. McRae that indigence creates an obstacle, sometimes even insuperable, to the assertion of certain rights.126 The majority of justices, however, firmly decline to take the next logical step. There is no constitutional restraint against stripping a citizen of the financial means to exercise a guaranteed right. (Recall that Mayer v. Roe the state wrote a new regulation to remove covered medical care if provided in connection with an abortion.) Medicaid and welfare spending rules can close the door to abortion in poor communities as tightly as if the procedure were a crime. The Court interprets that financial leverage as a neutral subsidy choice, implicating no constitutional right. As the majority reiterated in DeShaney v. Winnebago (1989), “the Due Process Clauses generally confer no affirmative right to governmental aid, even where such aid may be necessary to secure life, liberty, or property interests of which the government itself may not deprive the individual.”127 We are not opposed to carefully chosen litigation. We root for the good guys and rely on them to think carefully about the risks of an adverse decision. We predict, even so, that politics and policy will have to carry the main burdens of reform. That is as should be. Americans do not define our social compact by the barest minimum compliance with the Constitution. We express our values and priorities—our purpose, Beers might say—in acts of choice. The federal government, for all its solicitude for the rich, still offers support to the disabled, the elderly, and the unemployed alongside its gifts to real estate developers and hedge fund managers. A majority of voting-age Americans hold protection of the defenseless as a core value. That sense of justice, so innate that we display it in early childhood, can be marshaled in the cause of surveillance reform. There is room in a just society, as Dorothy Roberts has put it, for “not only the negative proscription against government coercion, but also the affirmative duty of government to protect the individual’s personhood from degradation and to facilitate the processes of choice and self-determination.”128 Defining appropriate boundaries here is no small task, but a right to privacy that covers the poor and disfavored will need to explore the terrain.

#### These aforementioned violations are terrible precedent and create legal harms

Toomey 18

Patrick Toomey, Senior Staff Attorney, ACLU National Security Project, The NSA Continues to Violate Americans' Internet Privacy Rights, Published by ACLU 8/22/18, <https://www.aclu.org/blog/national-security/privacy-and-surveillance/nsa-continues-violate-americans-internet-privacy)//LED>

A federal court will be scrutinizing one of the National Security Agency’s worst spying programs on Monday. The case has the potential to restore crucial privacy protections for the millions of Americans who use the internet to communicate with family, friends, and others overseas. The unconstitutional surveillance program at issue is called PRISM, under which the NSA, FBI, and CIA gather and search through Americans’ international emails, internet calls, and chats without obtaining a warrant. When Edward Snowden blew the whistle on PRISM in 2013, the program included at least nine major internet companies, including Facebook, Google, Apple, and Skype. Today, it very likely includes an even broader set of companies. PRISM Slide The government insists that it uses this program to target foreigners, but that’s only half the picture: In reality, it uses PRISM as a backdoor into Americans’ private communications, violating the Fourth Amendment on a massive scale. We don’t know the total number of Americans affected, even today, because the government has refused to provide any estimate. This type of unjustifiable secrecy has also helped the program evade public judicial review of its legality because the government almost never tells people that it spied on them without a warrant. Indeed, the government has a track record of failing to tell Americans about this spying even when the person is charged with a crime based on the surveillance. That’s one reason why this case is so important — this time, the government has admitted to the spying. In this case, the government accused a Brooklyn man, Agron Hasbajrami, of attempting to provide material support to a designated terrorist organization in Pakistan. After he pleaded guilty to one of the charges, the government belatedly admitted that it had read through his emails without a warrant. Now Mr. Hasbajrami has challenged the government’s warrantless surveillance and is asking the Second Circuit Court of Appeals to throw out the resulting evidence. The American Civil Liberties Union and the Electronic Frontier Foundation are supporting him as friends-of-the-court, arguing that the surveillance was unconstitutional (the brief we filed is here). At the hearing on Monday, we’ll explain to a three-judge panel why the Fourth Amendment requires the government to get a warrant when it wants to exploit the communications of Americans who are swept up in PRISM. This large-scale internet surveillance grew out of the Bush administration’s post-9/11 warrantless wiretapping program. It is conducted under a controversial law known as Section 702 of the Foreign Intelligence Surveillance Act. Relying on Section 702, the government intercepts billions of international communications — including many sent or received by Americans — and it hunts through them in investigations that have nothing to do with national security. The government attempts to defend this spying by pointing out that its “targets” are foreigners located abroad. But this is no defense at all. Americans regularly communicate with individuals overseas, and the government uses PRISM surveillance to collect and sift through many of these private communications. The government has even admitted that one of the purposes of Section 702 is to spy on Americans’ international communications without a warrant. The government casts a wide net, making it easy for innocent Americans who communicate with family, friends, and others overseas to be swept up. Relying on a single court order, the NSA uses Section 702 to put more than 125,000 targets under surveillance each year. These individuals need not be spies, terrorists, or accused of any wrongdoing — they can be journalists, business people, university researchers, or anyone else who may have information bearing remotely on “foreign affairs.” PRISM is a warrantless wiretapping program that operates around the clock, vacuuming up emails, Facebook messages, Google chats, Skype calls, and the like. Government agents do not review all of the information in real-time — there’s simply too much of it. Instead, the communications are pooled together and stored in massive NSA, FBI, and CIA databases that can be searched through for years to come, using querying tools that allow the government to extract and examine huge amounts of private information. PRISM Slide One of the most problematic elements of this surveillance is the government’s use of “backdoor searches” to investigate individual Americans. Although the government says PRISM is targeted at foreigners who lack Fourth Amendment privacy rights, it systematically combs through its PRISM databases for the emails and messages of Americans. Indeed, FBI agents around the country routinely search for the communications of specific Americans using their names or email addresses — including at the earliest stages of domestic criminal investigations. The result is an end-run around the Fourth Amendment. Investigators have easy access to a trove of Americans’ private emails, calls, and messages, without ever seeking individualized approval from any judge, as the Constitution requires. This surveillance leaves far too much unchecked power in the hands of executive branch officials. Today, that includes President Trump, who as a candidate called for expanded spying on Americans. The ACLU is taking on this threat to Americans’ privacy rights, just as we challenged the government’s warrantless wiretapping across both the Bush and Obama administrations. Now the courts must do their part to ensure that Americans’ online communications receive the full protection of the Fourth Amendment.

### Extensions

#### Massive reform necessary, it’s what minority leadership wants

Barton and Adler-Bell 17

Barton Gellman is an author, journalist and senior fellow at the Century Foundation, Sam Adler-Bell is a Century Foundation Contributor, The Disparate Impact of Surveillance, Published 12/21/17 by Century Foundation, <https://tcf.org/content/report/disparate-impact-surveillance/?session=1)//LED>

One important precondition of reform, in our view, is an intersectional approach to analysis, goal-setting, and policy instruments.129 This is not an empty slogan. Defining a universal right, if we want it to mean something practical, relies on a clear understanding of the particulars. Lawmakers and policy advocates are likelier to achieve the results they intend if they ask how any given proposal would interact with the real-world conditions of the rich and poor alike, man as well as woman, white as well as black, Christian as well as Muslim. Absent explicit attention to the disparate impact of surveillance tools, the liberal conception of general privacy not only leaves the disfavored behind, but also is likelier to fail on its own terms. The Fourth Amendment, to put the point lightly, already does a fine job of protecting white suburban men from stop-and-frisk and klieg lights aimed into their homes. We will have to think harder about how to bring that security to the urban poor. Initiatives such as the Color of Surveillance delegation, the Stop LAPD Spying Coalition, and the Movement for Black Lives (M4BL) are already engaged in a version of intersectional politics. The M4BL platform, which covers a far broader landscape, includes a demand for an end to the mass surveillance of black communities, and the end to the use of technologies that criminalize and target their communities (including IMSI catchers, drones, body cameras, and predictive policing software).130 The platform calls for reforms at the federal, state and local levels to address the specific harms of those tools and practices. Similarly, the Stop LAPD Spying Coalition describes itself as “committed to promoting and defending the human rights of multiple, interconnected groups of people, including but not limited to immigrants, youth, African Americans, Latinas, Muslims, LGBT communities, Indigenous and First Nation People, and all oppressed and marginalized communities.” Some reformers seek support from the privileged by portraying the unprivileged as test subjects for oppressive surveillance that may one day expand into the population at large. The argument is a well-intended effort to build a common sense of risk, but we believe it is a mistake. While it is true that aggressive new forms of are sometimes normalized over time—drones built for warfare overseas were repurposed to photograph migrants on the border, then used overhead at anti-Trump protests—too much is made of technology creep. The worst of the abuses we describe in this report are vanishingly unlikely to spill into whiter, richer, more privileged precincts where citizens have the power to fight back. There is no sense pretending otherwise, and no need: gross abuse of state power demands our attention whether or not it reaches us personally. There is no sense pretending otherwise, and no need: gross abuse of state power demands our attention whether or not it reaches us personally. An intersectional approach begins by observing the tangible effects of surveillance on the lives of real people. What disquiets us as we look ahead is the strong potential of new technologies, networked and integrated with the ones we have, to compound the harms of unequal treatment with new burdens on those citizens least capable of bearing them. Consider the potential impact of “Big Data,” a term that is more often invoked than explained. Big Data is shorthand for the marriage of sophisticated new computational techniques with inexpensive storage and off-the-shelf hardware that is faster and more capable than multi-million-dollar supercomputers from just a few years ago. Big Data offers even a mid-sized company the realistic prospect of acquiring and manipulating data sets on a national scale. For the U.S. government, which can buy just about any commercial data, collect a great deal more on its own, and then share large chunks of it with state and local authorities, there is no obvious limit. Artificial intelligence and machine learning spot patterns in data sets that no human could discern in a lifetime’s work. These capabilities offer great potential for good. They also provide the building blocks of the most consequential new surveillance machine since the smartphone. In application, Big Data techniques have already begun to amplify the disparate harms of surveillance in disfavored neighborhoods. Algorithmic analysis of historical crime data has begun a trend toward “predictive policing,” an aggressive focus on hypothetical future crime that existed only in science fiction until recently. Pouring law enforcement resources into historically over-policed communities, where the once-fashionable “broken windows” philosophy led to thousands of arrests for minor infractions, allows past injustice to define present policy. In Chicago, police have also mined Facebook and other social networks to identify individuals they judge to be at high risk of committing or becoming victims of gun violence. Even if these correlations sometimes prove out, the concentration of law enforcement power in “at risk” communities will reinforce the poisonous effects of historic biases. It aims to preempt bad acts by a small minority by subjecting all residents to aggressive law enforcement intrusions on the basis of their associations, demographics, and geography. Policy makers should give careful thought to that punitive impact on the blameless majority, which is exactly akin to the central grievance of the colonists against King George. As noted above, New York’s experiment with stop and frisk discovered firearms in 1.5 percent of its searches, many or most never used in a crime, at the cost of millions of searches that made up the other 98.5 percent. There is considerable risk that machine learning techniques, when applied to a statistical record of unequal policing, will reproduce that bias in the guise of neutral science. Prejudice embedded in computer code will be an exceptionally difficult question for lay policy makers to judge. Hamid Khan, the campaign coordinator of Stop LAPD Spying, has adapted an old programming aphorism to describe this risk: “It’s racism in, racism out.” Two Guiding Principles for Further Research and Advocacy Mitigating or preventing the harms of abusive surveillance may call for policies that are not typically considered under the rubric of privacy. Below we sketch two lines of further research and advocacy. Our purpose is not to write a comprehensive agenda. Our intent is to invite policy makers and privacy researchers into a conversation that takes disparities of power seriously in all its dimensions.

#### Massive impact

Munn 16

Nathan Munn is a CJFE contributor, HOW MASS SURVEILLANCE HARMS SOCIETIES AND INDIVIDUALS - AND WHAT YOU CAN DO ABOUT IT, Published by CJFE 11/8/16, https://www.cjfe.org/how\_mass\_surveillance\_harms\_societies\_and\_individuals\_and\_what\_you\_can\_do\_about\_it)//LED

For those of us who grew up in Canada, the idea that government security agents would one day be monitoring our movements, phone calls, text messages and internet activity seemed impossible. Today, however, we know that security agencies including the Canadian Security Intelligence Service (CSIS) and Communications Security Establishment (CSE), as well as local law enforcement agencies, are conducting unprecedented levels or surveillance on Canadians for a variety of purposes. We only know this is happening because of document leaks and government whistleblowers. While many people immediately recognize the problems that arise from this kind of mass surveillance, others have no issues with the practice. A common argument that skeptics use to brush off concerns about mass surveillance is that “only people who have something to hide” need to worry about it. This is a dangerous position to take for anyone who cares about democratic values, such as free expression, freedom of political affiliation and the right to privacy. Evidence shows that mass surveillance erodes intellectual freedom and damages the social fabric of affected societies; it also opens the door to flawed and illegal profiling of individuals. Mass surveillance has also been shown to not prevent terrorist attacks. Evidence shows that even the possibility of being under surveillance changes the way people think and act, causing them to avoid writing or talking about sensitive or controversial subjects—discussions that are necessary for the functioning of a free society. Beyond this ‘self-censorship’, the mass monitoring of citizens’ communications and movements achieves only one thing: the development of mutual mistrust between the individual and the state. ALTERED BEHAVIOUR So, how does mass surveillance affect the way we act? A 2016 study showed that people alter their behavior when they are reminded that the government is watching their activities. To test the effects of surveillance, participants in the study were first shown a fictional news headline about the United States targeting the Islamic State in an airstrike. They were then asked how they felt about the event while being regularly reminded that their responses were being monitored. As a result, most people in the study began to suppress opinions about the fictional event that they felt to be controversial or that they believed may lead to the government to scrutinize them. Interestingly, the study also showed that participants who support the idea of mass surveillance were the most likely to suppress their own non-conformist opinions. When it comes to creativity and the free expression of ideas, a survey conducted by PEN America in 2013 found that one in every six writers “has avoided writing or speaking on a topic they thought would subject them to surveillance.” Some analysts have pointed out that while journalists, activists and others who have already accepted the possibility of surveillance tend to continue their activities as before, people who are less politically engaged—oftentimes the average citizen—are more likely to self-censor and curb their involvement in any sort of activism as a result of ongoing surveillance. This chilling effect on participation in social causes and activities is an obvious threat to a functioning democracy. According to Glenn Greenwald, governments, corporations and other institutions of authority “crave surveillance…precisely because the possibility of being monitored radically changes individual and collective behavior,” leading to “fear and collective conformity.” Available evidence supports this claim. VISIT CJFE’S CAMPAIGN HEADQUARTERS TO LEARN MORE ABOUT SURVEILLANCE IN CANADA AND GET INVOLVED TODAY. DATA COLLECTION AND AGGREGATION Beyond its corrosive effects on intellectual curiosity and free speech, two extremely dangerous products of mass surveillance include the gathering and assembling of surveillance data to create individual profiles and to fuel predictive analysis. Security and law enforcement agencies aggregate surveillance data to create profiles of people and then attempt to predict their future behavior based on what they’ve done in the past. The problem with this practice is that it’s easy to make flawed presumptions and predictions based on data assembled in this ‘Frankenstein’ manner. These types of presumptions and biases are on display in so-called Crime Predicting software, which have been shown to disproportionately target poor and minority communities. While some of our security agencies have said they only collect “metadata” and not the contents of our communications, using metadata in an attempt to glean insights from people’s behavior has a high potential for abuse, especially as ever-increasing amounts of data are gathered and stored in ways beyond our control. The recent revelation that CSIS has been illegally storing metadata about Canadians only reinforces the seriousness of the current situation.

## Con

#### Framing:

Cost-Benefit Analysis; weigh impacts based on their net implications

### Contention: Domestic Terrorism

#### Domestic terror threat is at an all time high

Jones, Doxsee, and Harrington 20

Seth G. Jones; Harold Brown Chair; Director, Transnational Threats Project; and Senior Adviser, International Security Program, Catrina Doxsee Program Manager and Research Associate, Transnational Threats Project, Nicholas Harrington; Program Manager and Research Associate, Transnational Threats Project, The Escalating Terrorism Problem in the United States, Published by CSIS 6/17/20, <https://www.csis.org/analysis/escalating-terrorism-problem-united-states)//LED>

On June 3, 2020, federal authorities arrested three individuals allegedly associated with the “boogaloo” movement, a loosely-organized group of extremists preparing for a civil war, for conspiring to cause violence in Las Vegas and possessing an improvised incendiary device.1 Less than a week later, law enforcement officials near Richmond, VA, arrested Harry H. Rogers, a member of the Ku Klux Klan, for driving a vehicle into peaceful protesters. Around the same time, members of a Brooklyn anarchist group urged its supporters to conduct “rebellion” against the government.2 Extremists from all sides flooded social media with disinformation, conspiracy theories, and incitements to violence in response to the protests following the death of George Floyd, swamping Twitter, YouTube, Facebook, and other platforms.3 This CSIS brief examines the state of terrorism in the United States. It asks two sets of questions. First, what are the most significant types of terrorism in the United States, and how has the terrorism threat in the U.S. homeland evolved over time? Second, what are the implications for terrorism over the next year? To answer these questions, this analysis compiles and analyzes an original data set of 893 terrorist plots and attacks in the United States between January 1994 and May 2020. This analysis makes several arguments. First, far-right terrorism has significantly outpaced terrorism from other types of perpetrators, including from far-left networks and individuals inspired by the Islamic State and al-Qaeda. Right-wing attacks and plots account for the majority of all terrorist incidents in the United States since 1994, and the total number of right-wing attacks and plots has grown significantly during the past six years. Right-wing extremists perpetrated two thirds of the attacks and plots in the United States in 2019 and over 90 percent between January 1 and May 8, 2020. Second, terrorism in the United States will likely increase over the next year in response to several factors. One of the most concerning is the 2020 U.S. presidential election, before and after which extremists may resort to violence, depending on the outcome of the election. Far-right and far-left networks have used violence against each other at protests, raising the possibility of escalating violence during the election period. The rest of this brief is divided into the following sections. The first defines terrorism and its main types. The second section analyzes terrorism trends in the United States since 1994. The third examines far-right, far-left, and religious networks. The fourth section highlights the terrorism threat over the next year.

#### Time frame is now

Jones, Doxsee, and Harrington 20

Seth G. Jones; Harold Brown Chair; Director, Transnational Threats Project; and Senior Adviser, International Security Program, Catrina Doxsee Program Manager and Research Associate, Transnational Threats Project, Nicholas Harrington; Program Manager and Research Associate, Transnational Threats Project, The Escalating Terrorism Problem in the United States, Published by CSIS 6/17/20, <https://www.csis.org/analysis/escalating-terrorism-problem-united-states)//LED>

Our data suggest that right-wing extremists pose the most significant terrorism threat to the United States, based on annual terrorist events and fatalities. Over the next year, the threat of terrorism in the United States will likely increase based on several factors, such as the November 2020 presidential election and the response to the Covid-19 crisis. These factors are not the cause of terrorism, but they are events and developments likely to fuel anger and be co-opted by a small minority of extremists as a pretext for violence. First, the November 2020 presidential election will likely be a significant source of anger and polarization that increases the possibility of terrorism. Some—though not all—far-right extremists associate themselves with President Trump and may resort to violence before or after the election. As U.S. Department of Justice documents have highlighted, some far-right extremists have referred to themselves as “Trumpenkriegers”—or “fighters for Trump.”50 If President Trump loses the election, some extremists may use violence because they believe—however incorrectly—that there was fraud or that the election of Democratic candidate Joe Biden will undermine their extremist objectives. Alternatively, some on the far-left could resort to terrorism if President Trump is re-elected. In June 14, 2017, James Hodgkinson—a left-wing extremist—shot U.S. House Majority Whip Steve Scalise, U.S. Capitol Police officer Crystal Griner, congressional aide Zack Barth, and lobbyist Matt Mika in Alexandria, VA. A few months earlier, Hodgkinson wrote in a Facebook post that “Trump is a Traitor. Trump Has Destroyed Our Democracy. It’s Time to Destroy Trump & Co.”51 Tension on both the far right and far left has dramatically risen over the past several years. Second, developments associated with Covid-19—such as prolonged unemployment or government attempts to close “non-essential” businesses in response to a second or third wave—could increase the possibility of terrorism. Some far-right extremists, for example, have threatened violence and railed against federal, state, and local efforts to take away their freedoms by requiring face coverings in public indoor settings, closing businesses, and prohibiting large gatherings to curb the spread of the virus. In March 2020, Timothy Wilson, who had ties to neo-Nazi groups, was killed in a shootout with FBI agents who were attempting to arrest him for planning to bomb a hospital in Missouri. Though he had been planning the attack for some time and had considered a variety of targets, he used the outbreak of Covid-19 to target a hospital in order to gain additional publicity. On the far left and far right, some anti-vaxxers—who oppose vaccines as a conspiracy by the government and pharmaceutical companies—have threatened violence in response to Covid-19 response efforts.52 Third, a polarizing event other than the presidential election—such as a school shooting or racially-motivated killing—could spark protests that extremists attempt to hijack. As highlighted in the introduction, extremists from all sides attempted to hijack the May and June 2020 protests in the United States as an excuse to commit acts of terrorism. In addition, far-right and far-left networks have used violence against each other at protests—such as in Berkeley, CA and Charlottesville, VA in 2017—raising concerns about escalating violence. All parts of U.S. society have an important role to play in countering terrorism. Politicians need to encourage greater civility and refrain from incendiary language. Social media companies need to continue sustained efforts to fight hatred and terrorism on their platforms. Facebook, Google, Twitter, and other companies are already doing this. But the struggle will only get more difficult as the United States approaches the November 2020 presidential election—and even in its aftermath. Finally, the U.S. population needs to be more alert to disinformation, double-check their sources of information, and curb incendiary language. Terrorism feeds off lies, conspiracies, disinformation, and hatred. Indian leader Mahatma Gandhi urged individuals to practice what he called “satyagraha,” or truth force. “Satyagraha is a weapon of the strong; it admits of no violence under any circumstance whatever; and it always insists upon truth,” he explained.53 That advice is just as important as it has ever been in the United States.

#### Especially problematic is lone wolf terror

SPLC 15

Southern Poverty Law Center, SPLC REPORT: ‘LONE WOLF’ DOMESTIC TERRORISM ON THE RISE, Published by SPLC 2/12/15, <https://www.splcenter.org/news/2015/02/12/splc-report-%E2%80%98lone-wolf%E2%80%99-domestic-terrorism-rise)//LED>

As the White House prepares to host a major summit examining the threat of violent extremism next week, a Southern Poverty Law Center study of domestic terrorism released today finds that the vast majority of this violence is coming from “lone wolves” or “leaderless resistance” groups composed of no more than two people. As the White House prepares to host a major summit examining the threat of violent extremism next week, a Southern Poverty Law Center study of domestic terrorism released today finds that the vast majority of this violence is coming from “lone wolves” or “leaderless resistance” groups composed of no more than two people. The report – Age of the Wolf: A Study of the Rise of Lone Wolf and Leaderless Resistance Terrorism (download a PDF of the report)– examines more than 60 domestic terror incidents. Almost three-quarters of the incidents were carried out, or planned, by a lone wolf, a single person acting without accomplices. Ninety percent of the incidents were the work of no more than two persons. The study, which included violence from both the radical right and homegrown jihadists, also found that a domestic terrorist attack or foiled attack occurred, on average, every 34 days. It covered a period between April 1, 2009 and Feb. 1, 2015, and was based on records maintained by Indiana State University and the University of Maryland’s Global Terrorism Database, along with the SPLC’s own roster of apparent domestic terror incidents. “Our study clearly shows the urgent need for federal agencies to reinvigorate their work studying and analyzing the radical right,” said Mark Potok, SPLC senior fellow and editor of the report. “And it’s important to recognize the trend away from organized groups committing acts of domestic terror. As Timothy McVeigh demonstrated with the Oklahoma City bombing, lone wolves and small cells of domestic terrorists can create massive carnage.” The White House will hold a summit on Feb. 18 to examine the cycle of radicalization that spawns such extremists, but there is a danger, in the wake of the Charlie Hebdo attacks in France, that Islamist terror will become the focus. While jihadism is a deadly serious concern, the report shows that authorities should not focus on it to the exclusion of other threats. A timeline included with the report details a lengthy list of deadly attacks and plots across the country. They include a 2014 rampage in Nevada by a husband and wife with anti-government views that left two police officers and another man dead, a 2012 attack on a Wisconsin Sikh temple by a long-time neo-Nazi that killed six victims, and a 2010 attack that left an Internal Revenue Service (IRS) manager dead after a man who had attended radical anti-tax group meetings crashed his single-engine plane into an IRS office in Austin, Texas. “The lone wolf’s chief asset is that no one else knows of his violent plans, which makes them exceedingly difficult to disrupt,” Potok said. “It is imperative that authorities, including those gathering at the White House next week, take this threat seriously. Anything less would be an invitation to disaster.”

#### **NSA key to halt terror**

PARKINSON 13

JOHN R. PARKINSON, ABC Contributor, NSA: 'Over 50' Terror Plots Foiled by Data Dragnets, Published by ABC 6/18/13, <https://abcnews.go.com/Politics/nsa-director-50-potential-terrorist-attacks-thwarted-controversial/story?id=19428148)//LED>

June 18, 2013— -- The director of the National Security Administration today told Congress that more than 50 potential terrorist attacks have been thwarted by two controversial programs tracking more than a billion phone calls and vast swaths of Internet data each day. The attacks on would-be targets such as the New York Stock Exchange were prevented by caching telephone metadata and Internet information, including from millions of Americans since Sept. 11, 2001, Gen. Keith Alexander said during a hearing at the House Permanent Select Committee on Intelligence. Alexander had been less specific in testimony last week when he said "dozens" of possible attacks were foiled. He testified today: "In recent years, these programs, together with other intelligence, have protected the U.S and our allies from terrorist threats across the globe to include helping prevent the potential terrorist events over 50 times since 9/11." He appeared in a rare public hearing of the House Intelligence Committee with officials from the FBI and Justice Department to discuss the phone and Internet programs that were disclosed in June by former NSA contractor Edward Snowden in the British Guardian newspaper and also The Washington Post. Edward Snowden Says "I'm No Chinese Spy" Lawmakers had previously disclosed that about a dozen attacks were believed to have been thwarted as a result of the programs. Alexander said the full list of thwarted attacks will be provided to members of the House Intelligence committee Wednesday, but the intelligence community has decided to release only two of those events publicly. "If we give all those out, we give all the secrets of how we're tracking down the terrorists as a community," Alexander said. "And we can't do that." But he and other intelligence officials have pointed specifically to the case of Najibullah Zazi, the Afghan-born man who pleaded guilty in 2012 to plotting a terror attack against the New York City subway system. He is awaiting sentencing. More About Would-Be Bomber Najibullah Zazi FBI Deputy Director Sean Joyce testified today that "In the fall of 2009, NSA, using 702 authority [granted to intercept communication], intercepted an email from a terrorist located in Pakistan. That individual was talking with the individual located inside the United States talking about perfecting a recipe for explosives. "Through legal process, that individual was identified as Najibullah Zazi. He was located in Denver, Colorado. The FBI followed him to New York City. Later, we executed search warrants with the New York Joint Terrorism Task Force and NYPD and found bomb- making components and backpacks. Zazi later confessed to a plot to bomb the New York subway system with backpacks," Joyce said. The plot was previously disclosed. It has been argued by Snowden and others that the coded email message that foiled Zazi's plot could have been uncovered without the controversial PRISM electronic surveillance program, which apparently collects data from everyone for later dissection and not just suspected terrorists. Snowden, who has said he has more information to leak, accused administration officials and members of Congress in an online chat with The Guardian Monday of exaggerating claims about the success of the data collection programs in arresting terrorists, specifically New York subway bomb plotter Najibullah Zazi. The FBI's Joyce also said the NSA was able to provide the FBI with a previously unknown telephone number of Adis Medunjanin [who was convicted along with Zazi], which helped disrupt "the first core al Qaida plot since 9/11, directed from Pakistan." In today's newest revelation, he also said the NSA monitored a known extremist in Yemen, who was in contact with an individual in the United States, Khalid Ouazzan, which led to detection of "a nascent plot to bomb the New York Stock Exchange." Joyce also cited the case of David Headley, a U.S. citizen living in Chicago later convicted for his involvement in the 2008 Mumbai attacks in which more than 160 people died. Joyce said the NSA, through 702 coverage of an al Qaida-affiliated terrorist, found that Headley was working on a plot to bomb a Danish newspaper office that had published cartoon depictions of the prophet Muhammad. "Lastly, the FBI had opened an investigation shortly after 9/11," Joyce said, without further identifying specifics of the potential attack. "We did not have enough information nor did we find links to terrorism, so we shortly thereafter closed the investigation. "However, the NSA, using the business record FISA [Foreign Intelligence Surveillance Act], tipped us off that this individual had indirect contacts with a known terrorist overseas. We were able to reopen this investigation, identify additional individuals through a legal process and were able to disrupt this terrorist activity."

#### Surveillance metadata key to stop terror

Verhelst, Stannat, and Mecacci 20

H. M. Verhelst Delft Institute of Applied Mathematics, Delft University of Technology, , A. W. Stannat Delft Institute of Applied Mathematics, Delft University of Technology,, G. Mecacci Donders Institute for Brain, Cognition and Behaviour, Radboud University, Machine Learning Against Terrorism: How Big Data Collection and Analysis Influences the Privacy-Security Dilemma, Published by Springer 20, <https://link.springer.com/article/10.1007/s11948-020-00254-w)//LED>

When using a data set with a sufficient number of labelled cases, machine learning is able to assist law enforcement in detecting localised criminality, thus answering the question where and when crimes will be committed. However, when answering questions about who will commit a crime, in particular a terror attack, the features of datasets increase and data points are more distinct, leading to machine learning algorithms that are potentially less accurate. Well-known machine learning problems of class imbalance, the curse of dimensionality and spurious correlations lead us to believe there will be inaccuracies due to over- or underfitting. Consequently, the number of false positives and false negatives is expected to be very high when using these algorithms in enforcing national security, and general a priori uncertainty estimates of machine learning algorithms for the full population rather than the training set are currently missing. Furthermore, the use of metadata instead of data does not necessarily decrease the breaches of an individual’s privacy. Using studies from literature from the past decade, which all focussed on de-anonymisation of datasets on phone records, credit card data, cell phone locations and movie ratings, a careful evaluation of the actual anonymity of the available data is needed. In addition, the definition of metadata varies between systems, which means that metadata in one system is considered data in others. Due to this, it is important to carefully define the types of data intelligence agencies and third-parties are allowed to collect and share. We urge policymakers charged with evaluating the privacy-security dilemma to keep in mind the limitations of machine learning applied to mass-surveillance in the context of counterterrorism. With the increasing performance and accuracy of machine learning algorithms, we think that these techniques can assist law enforcement in finding patterns in properly fitted data sets, but at the same time they are far more intrusive. Considering the extreme sparsity of terror attacks and their versatility in planning and execution, we think that even with continuous progress in machine learning, training of the mass surveillance algorithms will be a challenge that should be evaluated carefully in the coming years against the consequences of big inaccuracies, and hence their effectiveness. Despite the fact that inaccuracies in current machine learning methods might entail opportunity costs related to human supervision, current technological hype might lead to over-adoption and consequent suboptimal resource allocation.

### Extensions

#### **Domestic terror comes from various groups, presents a large threat**

Jones, Doxsee, and Harrington 20

Seth G. Jones; Harold Brown Chair; Director, Transnational Threats Project; and Senior Adviser, International Security Program, Catrina Doxsee Program Manager and Research Associate, Transnational Threats Project, Nicholas Harrington; Program Manager and Research Associate, Transnational Threats Project, The Escalating Terrorism Problem in the United States, Published by CSIS 6/17/20, <https://www.csis.org/analysis/escalating-terrorism-problem-united-states)//LED>

There are three broad types of right-wing terrorist individuals and networks in the United States: white supremacists, anti-government extremists, and incels. There are numerous differences between (and even within) these types, such as ideology, capabilities, tactics, and level of threat. Adherents also tend to blend elements from each category. But there are some commonalities. First, terrorists in all of these categories operate under a decentralized model. The threats from these networks comes from individuals, not groups.12 For example, anti-government activist and white supremacist Louis Beam advocated for an organizational structure that he termed “leaderless resistance” to target the U.S. government.13 Second, these networks operate and organize to a great extent online, challenging law enforcement efforts to identify potential attackers.14 Right-wing terrorists have used various combinations of Facebook, Twitter, YouTube, Gab, Reddit, 4Chan, 8kun (formerly 8Chan), Endchan, Telegram, Vkontakte, MeWe, Discord, Wire, Twitch, and other online communication platforms. Internet and social media sites continue to host right-wing extremist ideas such as the Fourteen Words (also referred to as the 14 or 14/88) coined by white supremacist David Lane, a founding member of the group the Order. The Fourteen Words includes variations like: “We must secure the existence of our people and a future for white children.”15 Far-right perpetrators also use computer games and forums to recruit.16 Third, right-wing extremists have adopted some foreign terrorist organization tactics, though al-Qaeda and other groups have also adopted tactics developed by right-wing movements.17 In a June 2019 online post, a member of the Atomwaffen Division (AWD) stated, “the culture of martyrdom and insurgency within groups like the Taliban and ISIS is something to admire and reproduce in the neo-Nazi terror movement.”18 Similarly, the Base—a loosely organized neo-Nazi accelerationist movement which shares the English-language name for al-Qaeda—uses a vetting process to screen potential recruits, similar to the methods of al-Qaeda.19 This rise in right-wing activity is of national concern; it is not isolated to one region and affects cities of varying sizes. Figure 3 shows the locations of right-wing terror attacks and plots in the United States over the past six years. These incidents occurred in 42 states, Washington, DC, and Puerto Rico. White Supremacists: White supremacist networks are highly decentralized. Most believe that whites have their own culture that is superior to other cultures, are genetically superior to other peoples, and should exert dominance over others. Many white supremacists also adhere, in varying degrees, to the Great Replacement conspiracy. The conspiracy claims that whites are being eradicated by ethnic and racial minorities—including Jews and immigrants.20 Brenton Tarrant, the Christchurch shooter in New Zealand, and Patrick Crusius, the El Paso Walmart shooter, espoused the most radical view of the Great Replacement conspiracy, known as Accelerationism. As advocated by Tarrant and Crusius, violent accelerationists claim that the demise of Western governments should be accelerated to create radical social change and establish a whites-only ethnostate.21 White supremacists draw inspiration from individuals abroad and at home. Tarrant, for example, drew inspiration from Anders Breivik, who conducted the 2011 terrorist attack in Norway that killed 77 people, and Dylan Roof, who was responsible for the 2015 Charleston Church shooting that killed 9 people in South Carolina.22 Tarrant’s Christchurch attack then inspired terrorist attacks in the United States by John Earnest in California and Patrick Crusius in Texas.23 White supremacist actors have also travelled abroad seeking paramilitary training and networking opportunities. In Spring 2018, for example, members of the Rise Above Movement (RAM) travelled to Ukraine to celebrate Hitler’s birthday and train with the Azov Battalion, a paramilitary unit of the Ukrainian National Guard, which the FBI says is associated with neo-Nazi ideology.24 White supremacist neo-Nazi organizations, such as the Nationalist Socialist Movement, American Nazi Party, Vanguard America, and others often adhere to the Zionist Occupied Government (ZOG) conspiracy theory—that Jews secretly control the U.S. government, the media, banks, and the United Nations. Of particular concern is the emergence of the Atomwaffen Division (AWD), a U.S.-based neo-Nazi hate group with branches in the United Kingdom, Germany, and the Baltics.25 In January 2018, Brandon Russell, founder of the AWD was arrested and sentenced for possessing a destructive device and explosive material.26 Despite similar arrests, the AWD continues to plot, conduct attacks, and recruit. In February, four AWD members—including Cameron Shea, a high-level member and recruiter of the AWD—were arrested for conspiring to targets journalists and activists. They used encrypted chat platforms, distributed threatening posters, and wore disguises.27 Other arrests have been made under non-terrorism-related charges.28 The AWD continues to train and arm their members similar to international terrorist organizations. In January 2018, the AWD hosted a “Death Valley Hate Camp” in Las Vegas, Nevada, where members trained in hand-to-hand combat, firearms, and the creation of neo-Nazi propaganda videos and pictures. In August 2019, leadership members of the AWD attended a “Nuclear Congress” in Las Vegas, Nevada.29 Other white supremacist movements include the Base, the Patriot Front, and the Rise Above Movement.30 Anti-government Extremists: The right-wing terrorist threat also includes anti-government extremists, including militias and the sovereign citizen movement. Most militia extremists view the U.S. government as corrupt and a threat to freedom and rights.31 Other far-right anti-government groups mobilized to protect a perceived threat to individual gun ownership rights. Modern militias are organized as paramilitaries that conduct weapons training and other field exercises.32 The Three Percenters are a far-right paramilitary group that advocates gun rights and seeks to limit U.S. government authorities. In August 2017, Jerry Varnell, a 23-year-old who identified as holding the “III% ideology” and wanted to “start the next revolution” attempted to detonate a bomb outside of an Oklahoma bank, similar to the 1995 Oklahoma City bombing.33 Also, in January 2017, Marq Perez, who discussed the attack in Three Percenter channels on Facebook, burglarized and burned down a mosque in Texas.34 Anti-government extremists, which sometimes blend with white supremacist movements, have used the slang word “boogaloo” as a shorthand for a coming civil war. Several popular Facebook groups and Instagram pages, such as Thicc Boog Line, P A T R I O T Wave, and Boogaloo Nation, have emerged spreading the boogaloo conspiracy. Police in Texas arrested 36-year-old Aaron Swenson in April after he attempted to livestream his search for a police officer that he could ambush and execute.35 Prior to his arrest, Swenson had shared memes extensively from boogaloo pages. Incels: Involuntary celibates, or incels, conduct acts of violence against women. The incel movement is composed of a loosely organized virtual community of young males. Incels believe that one’s place in society is determined by physical characteristics and that women are responsible for this hierarchy. Incels identify with the writings of Elliot Rodger, who published a 133-page manifesto, titled “My Twisted World.”36 In October 2015, Christopher Harper-Mercer, inspired by Rodger, killed nine people at a community college in Oregon.37 In November 2018, 40-year-old Scott Beierle killed two women in a yoga studio in Tallahassee, Florida, before committing suicide.38 LEFT-WING TERRORISM The far-left includes a decentralized mix of actors. Anarchists are fundamentally opposed to a centralized government and capitalism, and they have organized plots and attacks against government, capitalist, and globalization targets.39 Environmental and animal rights groups, such as the Earth Liberation Front and Animal Liberation Front, have conducted small-scale attacks against businesses they perceive as exploiting the environment.40 In addition, the far-left includes Antifa, which is a contraction of the phrase “anti-fascist.” It refers to a decentralized network of far-left militants that oppose what they believe are fascist, racist, or otherwise right-wing extremists. While some consider Antifa a sub-set of anarchists, adherents frequently blend anarchist and communist views. One of the most common symbols used by Antifa combines the red flag of the 1917 Russian Revolution and the black flag of nineteenth-century anarchists. Antifa groups frequently conduct counter- protests to disrupt far-right gatherings and rallies. They often organize in black blocs (ad hoc gatherings of individuals that wear black clothing, ski masks, scarves, sunglasses, and other material to conceal their faces), use improvised explosive devices and other homemade weapons, and resort to vandalism. In addition, Antifa members organize their activities through social media, encrypted peer-to-peer networks, and encrypted messaging services such as Signal. Antifa groups have been increasingly active in protests and rallies over the past few years, especially ones that include far-right participants.41 In June 2016, for example, Antifa and other protestors confronted a neo-Nazi rally in Sacramento, CA, where at least five people were stabbed. In February, March, and April 2017, Antifa members attacked alt-right demonstrators at the University of California, Berkeley, using bricks, pipes, hammers, and homemade incendiary devices.42 In July 2019, William Van Spronsen, a self-proclaimed Antifa, attempted to bomb the U.S. Immigration and Customs Enforcement detention facility in Tacoma, Washington, using a propane tank but was killed by police.43

#### Right wing terror now

Spence 20

SEAN SPENCE, US News contributor, The New Wave of Global Terrorism Is Right-Wing Extremism, Published by US News 10/22/20, <https://www.usnews.com/news/best-countries/articles/2020-10-22/right-wing-extremism-the-new-wave-of-global-terrorism)//LED>

In April 2020, the United Nation's Secretary-General, António Guterres, addressed members of the Security Council by warning them that the COVID-19 pandemic could threaten global peace and security. [ READ: Climate Change Still Seen as Top Threat ] If the health crisis was not managed effectively, he feared that its negative economic consequences, along with a mismanaged government response, would provide an opportunity for white supremacists, right-wing extremists and others to promote division, social unrest and even violence to achieve their objectives. In early October 2020, less then a month before the United States federal election, the FBI thwarted an alleged terrorism plot by right-wing extremists to kidnap the Michigan governor, storm the state capital building and commit acts of violence against law enforcement. Photos You Should See - Oct. 2020 IRVINE, CALIFORNIA - OCTOBER 26: Firefighters work as the Silverado Fire burns toward a home in Orange County on October 26, 2020 in Irvine, California. The fire has prompted mandatory evacuations of 60,000 residents and has grown to 4,000 acres. (Photo by Mario Tama/Getty Images) View All 66 Images Their aim, according to court documents, was to start a "civil war leading to societal collapse." To date, 14 men have been arrested on charges of terrorism and other related crimes. Several of them are linked to the Wolverine Watchmen, a militia-type group in Michigan that espouses anti-government and anti-law enforcement views. The FBI recently briefed U.S. senators on the evolving concern of domestic violent extremists, groups whose ideological goals to commit violence stem from domestic influences such as social movements like #MeToo, Black Lives Matter and government policies. The composition of many of these organizations are right-wing terror groups whose grievances are rooted in racism, misogyny, anti-Semitism, anti-LGBTQ sentiments, Islamophobia and perceptions of government overreach. Given the wide range of grievances, these groups are defined as being complex, with overlapping viewpoints from similarly minded individuals advocating different but related ideologies. Toxic Masculinity Feminist researchers believe the rise of disenfranchised middle-class white males is leading to increased toxic masculinity within society, as evidenced by the increased popularity of the so-called manosphere to share extremist ideas and vent their grievances. Law enforcement agencies are concerned that the manosphere and similar online communities are radicalizing young men to commit violence to achieve their goals. This concern is valid, with plenty of evidence to support it. According to the University of Maryland's Global Terrorism Database, there were 310 terrorist attacks resulting in 316 deaths (excluding perpetrators) in the United States alone from 2015 to 2019. [ READ: Portland and Kenosha Violence Was Predictable – and Preventable ] Most were right-wing extremists, including white nationalists and other alt-right movement members. This alt-right movement also contains the incel (involuntary celibate) members who are a growing threat to women. But the increase in right-wing terrorism is not just a U.S. problem. The UN Security Council's Counterterrorism Committee says there's been a 320 per cent increase in right-wing terrorism globally in the five years prior to 2020. Recent terrorist attacks in New Zealand (2019), Germany (2019) and Norway (2019) are indicators of this trend. The Centre for Research on Extremism at the University of Oslo reports that both Spain and Greece are growing hotbeds for right-wing terrorism and violence. Canada isn't immune to these violent extremist ideologies. Many sympathizers to these causes reside in Canada, and as such there is always a risk for attacks. But the Canadian government is taking notice and has listed Combat 18 and Blood & Honour as right-wing terrorist organizations. A Major Global Security Threat Right-wing extremism is of such concern that when the top international security policy-makers met at the 2019 Munich Security Conference, they ranked it among space security, climate security and emerging technologies as the top global security threats. It would appear as though the world is at the dawn of a new age of terrorism that's different from before. Famed terrorism researcher David C. Rapoport argued in his influential thesis "The Four Waves of Rebel Terror and September 11" that modern terrorism can be categorized into four distinct waves. The first "Anarchist Wave" began in the 1880s in Russia with the Narodnaya Volya ("The People's Will") conducting assassinations of political leaders. It continued until the 1920s, spreading across the Balkans and eventually into the West, influencing the creation of new terror groups within different countries. The 1920s saw the beginning of the "Anti-Colonial Wave" coming out of the remnants of the First World War, when groups like the Irish Republican Army (IRA) began using ambush tactics against police and military targets to force political change. [ MORE: Al-Qaida: Fading Priority, Persistent Threat ] In the 1960s, the "New Left Wave" was created. This third wave emerged from the perceived oppression of Western countries within the developing world (like Vietnam and the Middle East). Its tactics included plane hijackings, embassy attacks and kidnappings perpetrated by groups like the Palestine Liberation Organization (PLO). Finally, the 1990s witnessed the birth of the "Religious Wave" in which terror groups like al-Qaida used religious ideology as a justification to overthrow secular governments with martyrdom tactics like suicide bombings. What all these waves have in common is that they last for a few decades and become infectious over time, spreading across the globe as new groups learn and adopt the successful tactics of previous ones. The Fifth Wave? This brings us to today's right-wing terrorism. Already observers have signalled the decline of violent Islamic movements and the rise of far-right extremist activities. Is right-wing violent extremism the new fifth wave of modern terrorism? If so, there's no doubt the negative societal impacts of COVID-19 will only help accelerate the radicalization of its adherents. And if the duration of the previous four waves have taught us anything, it's that this new one could be around for many more years to come.

NSA critical to halting terror

Mathes 15

Michael Mathes, AFP News contributor, CIA chief John Brennan, seen here on March 13, 2015, warned Sunday that allowing vital surveillance programs to expire could increase terror threats, Published by yahoo news, <https://news.yahoo.com/crunch-time-us-senate-nsa-spy-programs-set-173946541.html)//LED>

Washington (AFP) - CIA chief John Brennan warned Sunday that allowing vital surveillance programs to lapse could increase terror threats, as the US Senate scrambled to renew the controversial provisions hours before their expiration. With key counterterrorism programs under threat of suspension at midnight Sunday, the top intelligence official made a final pitch for Senate action, arguing that the bulk data collection of telephone records of millions of Americans unconnected to terrorism has not abused civil liberties and only serves to safeguard citizens. "This is something that we can't afford to do right now," Brennan said of allowing the counterterrorism provisions to expire at midnight Sunday. "Because if you look at the horrific terrorist attacks and violence being perpetrated around the globe, we need to keep our country safe, and our oceans are not keeping us safe the way they did century ago," he said on CBS talk show "Face the Nation." Brennan added that groups like Islamic State have followed the developments "very carefully" and are "looking for the seams to operate." The House has already passed a reform bill, the USA Freedom Act, that would end the telephone data dragnet by the National Security Agency and require a court order for the NSA to access specific records from the data retained by telecommunications companies. If no action is taken by the Senate Sunday, authorities will be forced to shut down the bulk collection program and two other provisions, which allow roving wiretaps of terror suspects and the tracking of lone-wolf suspects. A senior administration official said switches would be turned off for the bulk collection servers beginning at 3:59 pm (1959 GMT) Sunday, and any collection after midnight would be deemed illegal, without congressional authorization. "I do believe we have the votes" to pass the Freedom Act, Republican Senator Mike Lee, who supports ending NSA metadata collection, told CNN's State of the Union. "At this point I think the question is not about whether we will get it passed, but when." Senator Rand Paul, a Republican 2016 presidential candidate adamantly opposed to reauthorizing the surveillance, is threatening to use his parliamentary prerogative to delay votes on the reform bill or an extension of the original USA Patriot Act. That could force the counterterrorism provisions to lapse until Wednesday, and possibly later. - Political 'grandstanding' over security? - Brennan did not mention Paul by name, but he expressed exasperation over the politicization of important programs which he insisted "have not been abused" by US authorities. "Unfortunately I think there is a little too much political grandstanding and crusading for ideological causes that have really fuelled the debate on this issue," he said. The Senate meanwhile convened at 4:00 pm (2000 GMT) with the fate of the provisions hanging in the balance. Top Senate Democrat Harry Reid blasted Majority Leader Mitch McConnell for opposing the painstakingly crafted compromise reform legislation that overwhelmingly passed the House, but having no viable plan that would keep crucial provisions from expiring. "That's why we're here, staring down the barrel of yet another unnecessary manufactured crisis that threatens our national security," Reid said on the Senate floor. Senator Patrick Leahy, a senior Democrat who co-authored the Freedom Act, piled on, saying the Senate was facing a crises of McConnell's making. "We should pass it tonight," Leahy said of the reform bill. "But don't duck behind not doing anything and pretend that's a solution." McConnell stood at odds with House Speaker John Boehner, who warned how Al-Qaeda and IS could benefit if counterterror tools lapsed and urged the Senate to pass the Freedom Act. "Anyone who is satisfied with letting this critical intelligence capability go dark isn't taking the terrorist threat seriously," Boehner said Sunday. Independent Senator Angus King said it was important to halt the government storage of metadata, leaving it instead with telecommunications companies. But he said the Freedom Act should be improved so that it compels companies to hold data for a long period of time. "There should be some reasonable requirement for holding the data if, indeed, you think the program has value, and I do," King told CNN.