Watching the watchers: Mass Surveillance in the United States, United Kingdom, and France

Jacob Bourgault

Introduction

"We need a better way to handle our emotional responses to terrorism than by giving our government carte blanche to violate our freedoms, in some desperate attempt to feel safe again. If we don't find one, then, as they say, the terrorists will truly have won."[1]
– Bruce Schneier, American Cryptographer

Dr. Rahinah Ibrahim, a Muslim woman, is a Professor of Architecture at the Putra University of Malaysia.[2] Dr. Ibrahim lived in the United States for thirteen years pursuing higher education.[3] During that time, she received a Bachelor of Arts in Architecture from the University of Washington,[4] a Master of Architecture from the Southern California Institute of Architecture,[5] and was accepted into a Ph.D. program at Stanford University.[6] In early January 2005, during Ibrahim's studies at Standford, she had booked a flight to present her doctoral research.[7] While she was checking in, the airline staff found that she

---

[1] Bruce Schneier, Data and Goliath 228 (2016).

[2] *See* Rahinah Ibrahim, LinkedIn, https://my.linkedin.com/in/rahinah-ibrahim-1b1225b8 (last visited Feb. 17, 2025).

[3] Ibrahim v. U.S. Dep't of Homeland Sec., 912 F.3d 1147, 1154 (9th Cir. 2019) ("Dr. Ibrahim is a Muslim woman, scholar, wife, and mother of four children. She lived in the United States for thirteen years pursuing undergraduate and post-graduate studies.").

[4] *See* Ibrahim, *supra* note 2.

[5] *See id.*

[6] *See id.*

[7] *Ibrahim*, 912 F.3d at 1154 (noting that Dr. Ibrahim had "planned to fly from San Francisco to Hawaii" to "present the results of her doctoral research").

was on a No-Fly List.[8] The authorities were called and Ibrahim was arrested.[9] She was arrested in front of her fourteen year old daughter and in a wheelchair due to a previous operation.[10] She was then held for two hours and received no explanation from authorities for her detainment.[11]

Although Ibrahim was released and later permitted to fly back to Malaysia, she was unable to fly back to the United States when it came time to finish her doctoral degree: she was still on the No-Fly List.[12] Later that year, while still outside the U.S., her student visa was revoked.[13] The letter notifying Ibrahim of this decision cited a provision of the United States Code barring entry for those "reasonably believed to be engaged in or likely to be engaged in terrorist activity, or who has incited terrorist activity."[14] Dr. Ibrahim spent the next *eight years* trapped in a Kafkaesque set of proceedings that lacked clarity or a resolution to the issue.[15] In 2013, after "the government engaged in years of scorched earth litigation,"[16] it was later revealed that Ibrahim landed on the No-Fly List solely because an FBI agent misread a form.[17]

---

[8] *Id.* ("When Dr. Ibrahim arrived at the United Airlines counter, the airline staff discovered her name on the No Fly list and called the police.").

[9] *Id.* ("Dr. Ibrahim was handcuffed and arrested.").

[10] *See, e.g.*, *id.* ("Dr. Ibrahim arrived at SFO with her daughter, Rafeah, then fourteen. At the time, Dr. Ibrahim was still recovering from a hysterectomy performed three months earlier and required wheelchair assistance.").

[11] *Id.* ("[Ibrahim] was escorted to a police car (while handcuffed) and transported to a holding cell by male police officers, where she was searched for weapons and held for approximately two hours.... No one explained to Dr. Ibrahim the reasons for her arrest and detention.").

[12] *Id.* ("The next day [Ibrahim] returned to SFO where an unspecified person told her that she was again–or still–on the No Fly list. She was nonetheless allowed to fly.... [W]hen she arrived at the Kuala Lumpur International Airport, she was not permitted to board the flight to the United States.").

[13] *Id.* ("[O]n April 14, 2005, the U.S. Embassy in Kuala Lumpur wrote to inform Dr. Ibrahim that the Department of State had revoked her F-1 student visa on January 31, 2005....").

[14] *Id.* at 1155.

[15] *See generally id.* (discussing the prolonged immigration litigation against Ibrahim).

[16] *Id.* at 1171.

[17] Id. at 1157 ("Agent Kelley misunderstood the directions on the form and erroneously nominated Dr. Ibrahim to the TSA's No Fly list and DHS's IBIS. He did not intend to do so."); *see also* Maura Dolan, *Appeals Court Rebukes Federal Government in 'No-fly' Case, Ruling It Owes Millions in Legal Fees*, L.A. Times (Jan. 2, 2019), https://www.latimes.com/local/lanow/

All of this–the unjust arrest, eight-year litigation, and accompanying eight-year delay in her education–was due to a single agent misreading a single document. What happened to Dr. Ibrahim was likely driven, at least part, by U.S. law enforcement's mass surveillance of Muslims post-911. This widespread practice was engaged in by entities like the FBI,[18] New York Police Department,[19] and Los Angeles Police Department.[20] Yet, Muslims are not the only victims of mass surveillance in the United States. Nor is the practice of mass surveillance limited to the United States; places like the United Kingdom and France have also gone to great lengths to establish Orwellian surveillance states in the name of national security. The practices that led to Ibrahim's unfair treatment span across demographics, the United States, and the world.

This paper examines these government mass surveillance programs, focusing on the United States, the United Kingdom ("UK"), and France. This analysis includes *de jure* foreign intelligence surveillance practices (e.g., the legal basis for government surveillance in each jurisdiction) and *de facto* foreign intelligence surveillance practices (e.g., the surveillance systems that have actually been enacted, regardless of legality). The analysis reveals that these three countries have historically developed mass surveillance states. Civil unrest, foreign conflict, and public fear have driven the rise of mass surveillance infrastructure. Mass surveillance programs have often been conducted in secret, without appropriate oversight, and tend to be weaponized against minority groups. This analysis showed

---

la-me-ln-no-fly-terrorist-9thcircuit-20190102-story.html ("Ibrahim ended up on the no-fly list in 2004 because an FBI agent misread a form....").

[18] *See generally* Sabrina Alimahomed-Wilson, *When the FBI Knocks: Racialized State Surveillance of Muslims*, 45 Critical Socio. 871 (2019).

[19] *See* Saher Khan & Vignesh Ramachandran, *Post-9/11 Surveillance Has Left a Generation of Muslim Americans in a Shadow of Distrust and Fear*, PBS News (Sept. 16, 2021), https://www.pbs.org/newshour/nation/post-9-11-surveillance-has-left-a-generation-of-muslim-americans-in-a-shadow-of-distrust-and-fear (discussing NYPD and FBI surveillance of Muslims post-9/11).

[20] *See generally* Richard Winton et al., *LAPD Defends Muslim Mapping Effort*, L.A. Times (Nov. 10, 2007), https://www.latimes.com/local/la-me-lapd10nov10-story.html.

that, based on public knowledge, the U.S. has rolled back its mass surveillance efforts. However, mass surveillance in the UK and France is currently expanding. The history of these nation's mass surveillance efforts informs the papers' ultimate recommendations.

Part I defines mass surveillance for the purposes of this paper and the accompanying negative effects. Part II discusses the foreign intelligence surveillance practices of the United States, United Kingdom, and France. This includes a historical and contemporary analysis accompanied by constitutional provisions, legislation, case law, and surveillance infrastructure. Part III compares the historical and contemporary surveillance practices in each jurisdiction. Part IV briefly analyzes the costs and benefits of mass surveillance for foreign intelligence. Part V reconciles these values by making four proposals to maximize the benefits of foreign intelligence surveillance while minimizing the drawbacks. Part V calls for (1) three branch oversight of foreign intelligence surveillance with independent government watchdogs, (2) guaranteed privacy rights in each nation, (3) citizens to stand up for their privacy rights and civil liberties, even in times of fear, and (4) the tailored and safeguarded use of AI in surveillance efforts. The mass surveillance cycle must end and be replaced by targeted surveillance based on individualized suspicion.

People, generally, tend to exaggerate a sense of risk and focus on the worst-case scenario.[21] This susceptibility to fear can lead people to give up their civil liberties for a feeling of temporary security.[22] But this susceptibility to fear, and the accompanying consequences, are misguided. Sacrificing one's civil liberties–in the case of mass surveillance, the privacy rights of millions–leads to an abridgement of those individuals' fundamental needs, gives unfettered discretion and power to the government, and risks the possibility of unjust results, particularly against marginalized groups. While the negative effects of mass

[21] See generally Cass R. Sunstein, Fear and Liberty, 71 Soc. Rsch. 967 (2004).

[22] *See id.* at 967 ("In the midst of external threats, public overreactions are predictable. Simply because of fear, the public and its leaders will favor measures that do little to protect security but that compromise important forms of freedom.").

surveillance are *salient* and *recurring*, they are nonetheless allowed to fester so that *nebulous* national security interests can be protected. Namely, the governments' national security interest in attempting to prevent speculative attacks that may never happen and, even if it were to happen, may not have been caught through mass surveillance.[23] To break this wheel in the early age of Artificial Intelligence ("AI"), which has the possibility to exasperate this surveillance, it is critical to first examine where mass surveillance has been–and where it is headed.

I. DEFINING "MASS SURVEILLANCE" AND NEGATIVE EFFECTS

Although mass surveillance can be defined a number of ways, this paper adopts the definition posed by Amnesty International: "Indiscriminate mass surveillance is the monitoring of internet and phone communications of large numbers of people – sometimes entire countries – without sufficient evidence of wrongdoing."[24] This definition excludes things like the Lantern Laws in the United States (which predated the constitution, and required slaves to carry lit lanterns if unaccompanied by a white person) and recording of information in the national census.[25] This definition was chosen because of its contemporary relevance. Under this definition, things like wiretapping a single individual–or small group of individuals–under investigation for a specific crime is excluded. Instead, this paper focuses on country or demographic wide surveillance practices focused on intercepting

[23] This argument is expanded upon *infra* Part IV.

[24] *Easy Guide to Mass Surveillance*, Amnesty Int'l, https://www.amnesty.org/en/latest/campaigns/2015/03/easy-guide-to-mass-surveillance (last visited Feb. 17, 2025).

[25] *See History of Surveillance Timeline*, Univ. Mich.: Info. & Tech. Servs. [hereinafter *U.S. Surveillance Timeline*], https://safecomputing.umich.edu/protect-privacy/history-of-surveillance-timeline (last visited Feb. 17, 2025) ("Lantern Laws in New York City in the 1700s require Black, mixed-race, and Indigenous enslaved people to carry lit lanterns when in the city after sundown and unaccompanied by a white person.").

foreign intelligence. Several countries, including the three in this analysis, have aimed to surveil broad swaths of their populations.

Dr. Ibrahim's story, and those like it, help to show why the mantra "I have nothing to hide" is an insufficient resolution to surveillance states. Nor is surveillance, in and of itself, harmless. The right to privacy is something that, like other civil liberties, shields citizens from abuses of power and is a fundamental need for individuals.[26] Individuals need community and socialization, but they similarly need to be able to withdraw from others and not have their personal space or correspondence invaded.[27] This need for privacy is found in other non-human animals.[28] Biologist and author Peter Watts notes that "Mammals don't respond well to surveillance. We consider it a threat. It makes us paranoid, and aggressive and vengeful.... The link between surveillance and fear is a lot deeper than the average privacy advocate is willing to admit."[29] Humans have long recognized this need, as "practices designed to protect privacy are found in almost all societies, across time and geographies."[30] The right to privacy is important enough that it is codified in both the United Nations' Universal Declaration of Human Rights[31] and European Convention on Human Rights ("ECHR").[32]

---

[26] *See* Carissa Véliz, *The Ethics of Privacy and Surveillance*, Inst. for Ethics in AI (Jan. 23, 2024), https://www.oxford-aiethics.ox.ac.uk/blog/new-book-ethics-privacy-and-surveillance ("Privacy matters because it shields us from possible abuses of power. Human beings need privacy just as much as they need community.").

[27] *See id.* ("Our need for socialization brings with it risks and burdens which in turn give rise to the need for spaces and time away from others.").

[28] *See id.* (noting that things like "the need to withdraw from others, the ability to deceive, the desire to save face, and the tendency to feel uncomfortable when others stare" are privacy traits found in "human beings and some non-human animals alike").

[29] *Peter Watts on the Harms of Surveillance*, Schneier on Sec. (May 23, 2014), https://www.schneier.com/blog/archives/2014/05/alan_watts_on_t.html.

[30] Véliz, *supra* note 26.

[31] G.A. Res. 217 (III) A, Universal Declaration of Human Rights Art. 12 (Dec. 10, 1948) ("No one shall be subjected to *arbitrary interference with his privacy, family, home or correspondence*, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks." (emphasis added)).

[32] European Convention on Human Rights art. 8 ("Everyone has the *right to respect for his private and family life*, his home and his correspondence." (emphasis added)).

Still, some scholars have posed that mass surveillance is harmless. These scholars take the position that if you have nothing to hide, then it does not affect you while simultaneously keeping people safe.[33] However, this argument has three underlying faults: (1) it neglects to consider that privacy violations are inherently harmful to individuals; (2) surveillance often leads to mistakes and perpetuates oppression against marginalized groups, as seen in Dr. Ibrahim's previously delineated story; and (3) mass surveillance has proven ineffective for protecting national security, undermining national interests by diverting resources from more effective programs.[34] Neil Richards, a law professor at Washington University in St. Louis, takes a different tack. Richards argues that surveillance is inherently harmful because it threatens "intellectual privacy."[35]

Richards takes the position "that people should be able to make up their minds at times and places of their own choosing; and that a meaningful guarantee of privacy – protection from surveillance or interference – is necessary to promote this kind of intellectual freedom."[36] He presents a (1) normative and (2) empirical basis for the argument. The normative basis is that civil liberties should protect the right to form beliefs through reading, thinking, and having private conversations.[37] This is undermined when people have to worry about the government snooping on their private correspondence and activities. The empirical basis examines empirical studies and popular media to conclude that

---

[33] *See, e.g.*, Dr. Gabriel Schoenfeld, *In Defense of the American Surveillance State*, 63 Drake L. Rev. 1121, 1134 (2015) ("The measures taken to interdict terrorist communication deserve applause, not condemnation. The American surveillance state is working pretty well.... There has not been a reprise of 9/11.").

[34] For a more detailed discussion of the ineffectiveness of mass surveillance, see *infra* Part IV.

[35] Neil M. Richards, *The Dangers of Surveillance*, 126 Harv. L. Rev. 1934, 1945 (2013) ("The most salient harm of surveillance is that it threatens a value I have elsewhere called 'intellectual privacy.'").

[36] *Id.* at 1496.

[37] Id. ("The normative claim is that the foundation of Anglo-American civil liberties is our commitment to free and unfettered thought and belief – that free citizens should be able to make up their own minds about ideas big and small, political and trivial. This claim requires at a minimum protecting individuals' rights to think and read, as well as the social practice of private consultation with confidantes.").

surveillance undermines "our society's foundational commitments to intellectual diversity and eccentric individuality" by preventing people from engaging in actions or thoughts that are outside the norm.[38] Richards also notes that surveillance in the U.S has led to blackmail (e.g., the FBI admitting to attempting to blackmail Martin Luther King Jr. in an effort to silence his civil rights activism), government persuasion, and discrimination.[39]

Others have also studied empirical data showing the harms of mass surveillance. Daragh Murray et al. recently examined the effects of AI-empowered mass surveillance in Uganda and Zimbabwe.[40] The empirical analysis found that mass surveillance increased self--censorship, led to intimidation-induced chilling effects on speech, and undermined the freedom of assembly.[41] This study found that mass surveillance had tangible negative effects (e.g., fear and distrust among the population) as well as the intangible negative effects (e.g., loss of public discourse and engagement between different groups).[42] Similarly, a poll in the United States found that 88% of those surveyed felt "it is important that they not have someone watch or listen to them without their permission."[43] Further, just 6% felt confident that government agencies could keep their records secure.[44] After the Snowden leaks, the Parliamentary Assembly of the Council of Europe cited a study concluding that 85% of U.S. writers feared government surveillance, leading many to self-censor.[45]

---

[38] *Id.* at 1948.

[39] *Id.* at 1953–58 (discussing "Blackmail," "Persuasion," and "Sorting/Discrimination" as negative effects of mass surveillance).

[40] Daragh Murray et al., *The Chilling Effects of Surveillance and Human Rights: Insights from Qualitative Research in Uganda and Zimbabwe*, 16 J. Hum. Rts. Prac. 397 (July 31, 2023).

[41] *Id.* at 403 –09 (delineating the effect of mass surveillance on the examined communities).

[42] *Id.* (same).

[43] Mary Madden & Lee Rainie, *Americans' Attitudes About Privacy, Security and Surveillance*, Pew Rsch. Ctr. (May 20, 2015), https://www.pewresearch.org/internet/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance.

[44] *Id.* ("Just 6% of adults say they are 'very confident' that government agencies can keep their records private and secure....").

[45] Eur. Parl. Ass., Comm. On Legal Affs. & Hum. Rts., *Mass Surveillance* at 25 (2015), https://

Based on Western norms regarding civil liberties and empirical data, mass surveillance has proven harmful. Of course, many people are likely to be cognizant of this fact. Privacy, as previously mentioned, is fundamental to humans. However, so is safety and a feeling of comfort. Striking this balance is part of the reason that mass surveillance has been allowed to continue. In 2014, the world's oldest defense think-tank went as far as concluding that "[t]here seems to be a political consensus on the need for surveillance of digital data that is proportionate to the danger faced by UK citizens."[46] However, the think tank did not cite any empirical evidence to support this, instead pointing to two speeches by UK politicians.[47] Still, this balance between national security, privacy rights, and other civil liberties has underpinned every argument for and against mass surveillance throughout history.

II. THE RIGHT TO PRIVACY AND MASS SURVEILLANCE

This section examines the evolution of mass surveillance practices in the U.S., UK, and France. It is worth noting preliminarily that the United States is considerably younger than either the UK or France. Detailing the full evolution of the UK and France's surveillance practices throughout their history would take the balance of the paper to reproduce. For example, the earliest attempt at mass surveillance among these countries may have been William the Conqueror's Domesday Book in 1086.[48] The Domesday Book served as a pseudo-census and is

www.scribd.com/document/253848295/Mass-Surveillance-Report ("85% of the 520 American writers who responded to the survey said they are worried about government surveillance.").

[46] Commentary, *The Politics of Surveillance*, Royal United Servs. Inst. for Def. & Sec. Stud. (Mar. 7, 2014), https://rusi.org/explore-our-research/publications/commentary/politics-surveillance.

[47] *See generally id.*

[48] *See* Dr. Gary Girod, *Mass Surveillance in France & Britain: The Aristocratic Age*, Fr. Hist. Podcast (May 31, 2024), https://www.thefrenchhistorypodcast.com/mass-surveillance-in-france--britain-the-aristocratic-age ("The earliest attempt at widespread intelligence-gathering by the central state as a means of controlling the population in England was the Domesday Book 1086....").

considered the "earliest attempt at widespread intelligence-gathering by the central state as a means of controlling the population in England."[49] Since synthesizing the entire history of each countries surveillance practices is impracticable, this paper focuses on government mass surveillance of foreign intelligence conducted by these three countries since the late 18th century. This coincides with the founding of the United States. It is important to note that discussions on the Five Eyes program, which includes both the U.S. and UK, are saved for the UK section.

Each country's section is divided into three parts: Pre-World War I, World War I to the 21st Century, and the Contemporary Era. As this paper shows, the implementation of mass surveillance and foreign intelligence programs are often the result of domestic unrest or international conflict. Both World Wars and 21st-century terrorism catalyzed the development of mass surveillance infrastructure. It is because of these developments that these three periods were chosen. The first section focuses on the youngest country in this analysis, the United States.

A. United States

Modern understandings of foreign intelligence surveillance in the U.S. are closely tied to the National Security Agency's ("NSA") mass surveillance, the post-911 Patriot Act, and Edward Snowden's leaks. However, in order to understand how this contemporary framework came about, it is important to examine the evolution of U.S. government surveillance practices. Part II.A.1 examines foreign intelligence surveillance from America's founding to WWI. Foreign intelligence played a key role in the Revolutionary War, Civil War, and George Washington's presidency, but lagged behind the practices of the UK and France at the time. Part II.A.2 examines WWI to the 21st century. During that time, several government operations sought to spy on domestic Americans and foreigners. This period also saw the development of increased surveillance capabilities during WWII, as well as a

[49] *Id.*

combination of bills and an executive order that established the framework underpinning modern mass surveillance. Finally, Part II.A.3 examines the contemporary framework.

1. Pre-WWI

While the capabilities accompanying contemporary mass surveillance are relatively recent developments, tracking and monitoring people is not. Indeed, surveillance in its earliest form was enacted through the 1700's New York Lantern Laws, preventing slaves from walking at night unaccompanied unless they had a lantern.[50] Foreign intelligence also played a key role in the Revolutionary War against the British. George Washington developed spy rings to report on British troop movements.[51] The Continental Congress established the Committee of Secret Correspondence in 1775 to gather information from Europeans to help the war effort.[52] During George Washington's presidency, he continued to focus on the importance of intelligence and requested intelligence funding from Congress.[53] By the third year of his presidency intelligence funding accounted for approximately "12% of the Government's budget."[54]

Although federal foreign intelligence surveillance would falter after Washington' presidency, states and private parties occasionally

---

[50] *See, e.g.*, Zain Murdock, *These Lantern Laws Laid The Groundwork For Modern-Day Surveillance And Stop-And-Frisk*, PushBlack (June 28, 2023), https://www.pushblack.us/news/these-lantern-laws-laid-groundwork-modern-day-surveillance-and-stop-and-frisk (noting that the New York law forbade any "Negro or Indian Slave... to be... in any of the streets... without a lanthorn.").

[51] *See The Evolution of the U.S. Intelligence Community-An Historical Overview*, GovInfo, https://www.govinfo.gov/content/pkg/GPO-INTELLIGENCE/html/int022.html (last visited Feb. 27, 2025) ("Washington recruited and ran a number of agents, set up spy rings, devised secret methods of reporting, analyzed the raw intelligence gathered by his agents, and mounted an extensive campaign to deceive the British armies.")

[52] *See id.* ("In November of 1775, the Continental Congress created the Committee of Secret Correspondence to gather foreign intelligence from people in England, Ireland, and elsewhere on the European continent to help in the prosecution of the war.").

[53] *See id.* ("Washington's keen interest in intelligence carried over to his presidency.... Washington asked the Congress for funds to finance intelligence operations.").

[54] *Id.*

formed their own surveillance programs. In 1819, South Carolina enacted legislation requiring all white men over 18 to track and regulate the activity of slaves.[55] One of the first private surveillance practices came from Pinkerton's National Detective Agency ("Pinkerton's"), which still exists today under the name Pinkerton Consulting & Investigations, Inc.[56] In the mid-1800s Pinkerton's conducted surveillance on criminal and labor organizers on behalf of the U.S. government, with Allan Pinkerton becoming the "the first to form an intelligence service for the federal government."[57] Foreign intelligence surveillance would later see a federal revitalization during the Civil War.

During the Civil War, from 1861-1865, the Union intercepted telegraphs and mail from the Confederacy.[58] Both sides established intelligence surveillance systems, as well as spy networks.[59] The Union's surveillance efforts allowed them to track Confederate troop movements and decode confederate message over telegraph.[60] These surveillance efforts greatly assisted the Union in winning the war.[61] Approximately 20 years later, in the 1880s, the Office of Naval Intelligence and the Military Intelligence Division were formed to monitor foreign and domestic military intelligence.[62] From the 1880s until WWI, U.S.

---

[55] *U.S. Surveillance Timeline*, *supra* note 25 (noting that in 1819 "[t]he South Carolina General Assembly enact[ed] a law requiring all white men over the age of 18 to participate in slave patrols").

[56] *See generally Our History*, Pinkerton Consulting & Investigations, Inc., https://pinkerton.com/our-story/history.

[57] Alan Bilansky, *Pinkerton's National Detective Agency and the Information Work of the Nineteenth-Century Surveillance State*, 53 Info. & Culture 67, 79 (2018).

[58] *See, e.g.*, *19th Century – The Origins of Surveillance*, Stan. Univ., https://cs.stanford.edu/people/eroberts/cs181/projects/ethics-of-surveillance/history_19century.html (last visited Feb. 17, 2025) ("Wiretapping was perhaps the earliest form of surveillance and began during the Civil War when both the Union and the Confederacy tapped into each other's telegraph lines and copied down the messages.").

[59] *See* GovInfo, *supra* note 51 ("Both the Union and Confederate leadership valued intelligence information, established their own spy networks, and often railed at the press for providing intelligence to the other side.").

[60] *See id.* (noting that Union surveillance efforts led to successfully "detecting a large concentration of Confederate troops preparing to attack at Fair Oaks, Virginia").

[61] *See generally id.*

[62] *See id.* (noting that the Office of Naval Intelligence was created in March 1882, and the Military Intelligence Division was created three years later).

surveillance activities were primarily focused on domestic intelligence.[63] This included the Justice Department's Bureau of Investigation, the predecessor to the Federal Bureau of Investigations ("FBI"), being formed in 1908 due to concerns that the federal government was spying on members of Congress.[64]

However, prior to the breakout of WWI, the United States lacked comprehensive and coordinated intelligence efforts.[65] This was likely in part due to President Woodrow Wilson's (1913-1921) disdain for spies and surveillance, instead preferring open diplomacy.[66] However, British intelligence services would contribute to the U.S. entering the war and, eventually, the development of U.S. intelligence infrastructure. The British intercepted German intelligence revealing that the Germans were attempting to prevent the U.S. from contributing finance or goods to the British war effort.[67] A catalyst for the U.S. entering WWI was the British interception of the "Zimmerman Telegram," which promised Mexico land from the U.S. if they joined the Germans.[68] This "wake-up" call for President Wilson led the U.S. into WWI and, as an accompanying result, the development of increased U.S. surveillance infrastructure.

---

[63] *See id.* ("For the most part, however, the early part of the twentieth century was marked not by an expanded use of intelligence for foreign policy purposes, but by an expansion of domestic intelligence capabilities.").

[64] *See id.* ("The Justice Department's Bureau of Investigation (the forerunner of the FBI) was established in 1908 out of concern that Secret Service agents were spying on members of Congress.").

[65] *See id.* ("At the time the United States entered [World War I], it lacked a coordinated intelligence effort.").

[66] *See id.* ("As a champion of open diplomacy, President Woodrow Wilson had disdained the use of spies and was generally suspicious of intelligence.").

[67] *See id.* ("British intelligence played a major role in bringing the United States into World War I. Public revelations of German intelligence attempts to prevent U.S. industry and the financial sector from assisting Great Britain greatly angered the American public.").

[68] *The Zimmermann Telegram*, Nat'l Archives (June 2, 2021), https://www.archives.gov/education/lessons/zimmermann ("In January 1917, British cryptographers deciphered a telegram from German Foreign Minister Arthur Zimmermann to the German Minister to Mexico, Heinrich von Eckhardt, offering United States territory to Mexico in return for joining the German cause. This message helped draw the United States into the war and thus changed the course of history.").

2. WWI to 21st Century

WWI led to the formation of MI-8 in 1917. MI-8 was mandated to decode military communications and ensure the security of the army's correspondence.[69] This data was transferred to the state department and would later becoming known as the "Black Chamber."[70] The Black Chamber monitored intelligence even after the war ended, including from Japanese officials in the early 1920's.[71] MI-8 and the Black Chambers surveillance efforts would be derailed by President Herbert Hoover (1929-1933), who shared President Wilson's distaste for snooping on private correspondence.

Domestically, wiretapping was the primary surveillance mechanism, but would not be widely used by U.S. law enforcement until Prohibition in the 1920s-30s.[72] Even still, the NYPD had a national scandal in 1916 when they were caught wiretapping "hundreds of phones a year to track criminals and suppress labor activism."[73] These developments did not lead to any major policy changes and the 1928 Supreme Court, in a narrow 5-4 vote, held that wiretapping without a warrant was not a constitutional violation.[74] Further, The Espionage Act of 1917 and Palmer Raids accompanying the Red Scare both led to government monitoring of private actors based on potential political affiliations.[75] The former targeted disloyalty in the First World War, and

---

[69] *See* GovInfo, *supra* note 51 ("In June of 1917, the first U.S. signals intelligence agency was formed within the Army. Known as 'MI-8,' the agency was charged with decoding military communications and providing codes for use by the U.S. military.").

[70] *See id.*

[71] *See id.* ("In 1921, the Black Chamber celebrated perhaps its most significant success by decrypting certain Japanese diplomatic traffic.").

[72] *See* April White, *A Brief History of Surveillance in America*, Smithsonian Mag. (Apr. 2018), https://www.smithsonianmag.com/history/brief-history-surveillance-america-180968399 ("Until the 1920s, wiretapping was most often used by private detectives and corporations. It wasn't until Prohibition that it became a common law enforcement tool.").

[73] *U.S. Surveillance Timeline*, *supra* note 25.

[74] Olmstead v. United States, 277 U.S. 438 (1928).

[75] *U.S. Surveillance Timeline*, *supra* note 25 ("Following World War I and the Russian Revolution of 1917, the first Red Scare period in the United States was marked by fear of leftist movements and influence. The U.S. Department of Justice conducted raids led by Attorney General A. Mitchell Palmer, known as Palmer Raids in an attempt to arrest foreign anarchists, commu-

the latter targeted potential communist sympathizers (surveillance that would be reprised during the Cold War).[76] In the late years of WWI, Congress enacted the Sedition Act of 1918, which made it a crime to "willfully utter, print, write, or publish any disloyal, profane, scurrilous, or abusive language about the form of Government of the United States."[77] Interestingly, by the 1960s U.S. citizens supported wiretapping for national security purposes, but opposed its use in criminal matters (a perspective that has now largely flipped).[78]

It was during World War II that the U.S. began to enact much of its mass surveillance, generally focusing on communist sympathizers. In 1938, the House Un-American Activities Committee ("HUAC") was created to investigate and track communist sympathizers.[79] In 1945 the United States began Project SHAMROCK out of the ashes of, and largely because of, WWII.[80] Project SHAMROCK monitored domestic radio and wire communications with foreign entities, collecting "approximately 150,000 messages per month" at its peak.[81] This program lasted

---

nists, and radical leftists.").

[76] History.com Editors, *Red Scare*, History (Apr. 21, 2023), https://www.history.com/topics/cold-war/red-scare#cold-war-concerns-about-communism (delineating the first Red Scare (1917--1920) and subsequent Red Scare during the Cold War).

[77] *The Sedition Act of 1918*, Digit. Hist. (2021), https://www.digitalhistory.uh.edu/disp_textbook.cfm?smtID=3&psid=3903.

[78] White, *supra* note 72 ("By 1965, the normative political position in the United States was that wiretapping for national security was a necessary evil, whereas wiretapping in the service of the enforcement of criminal law–in, say, tax evasion cases or even in Mafia prosecutions, which was a big priority among American law enforcement starting in the 1960s–was outrageous and an abuse of power. Today, it's the opposite. Most people are worried about wiretapping by the government.").

[79] *See House Un-American Activities Committee*, Harry S. Truman Libr., https://www.trumanlibrary.gov/education/presidential-inquiries/house-un-american-activities-committee (last visited Feb. 17, 2025) ("HUAC was created in 1938 to investigate alleged disloyalty and rebel activities on the part of private citizens, public employees and organizations suspected of having Communist ties.").

[80] Major Dave Owen, A Review of Intelligence Oversight Failure: NSA Programs that Affected Americans 33 (2012), https://irp.fas.org/agency/army/mipb/2012_04-owen.pdf ("Project SHAMROCK began in August 1945, shortly before the end of World War II and over seven years prior to the establishment of the NSA.").

[81] *Id.* at 34; *see also U.S. Surveillance Timeline*, *supra* note 25 ("Operation SHAMROCK was tasked with monitoring radio and wire communications targeting agents of foreign governments or agents of foreign commercial enterprises.").

until the 1970s,[82] and is an early example of the U.S. government conducting a large-scale collection and analyzation of American citizens private correspondence.[83]

The 1947 National Security Act led to the development of the National Security Council ("NSC") and Central Intelligence Agency ("CIA").[84] Just five years later, and what is now a household name after Edward Snowden's leaks, the National Security Agency ("NSA") was formed as an agency largely unknown to the public.[85] Contemporaneously, the FBI began its Counterintelligence Program ("COINTELPRO") which "expanded its domestic surveillance programs" and tracked communists, socialists, and black civil rights groups.[86] The NSA's first major mass surveillance program came around this time and was called Project MINARET.[87] Integrating data from Project SHAMROCK, Project MINARET cataloged the actions of American citizens and put certain people on a "watch list."[88] This list targeted "individuals and

---

[82] *See, e.g.*, Owen, *supra* note 80, at 34 ("The Director of the NSA terminated Project SHAMROCK in 1975....")

[83] *Cf.* ("Though Project SHAMROCK undoubtedly collected and analyzed American citizens' private communications on a large scale, this effort still focused on foreign intelligence.").

[84] *National Security Act of 1947*, U.S. Dep't State: Off. Hist., https://history.state.gov/milestones/

1945-1952/national-security-act (noting that the National Security Act of 1947 created both the NSC and CIA).

[85] *See, e.g.*, Owen, *supra* note 80, at 33 ("President Truman created NSA in 1952.... [S]ince both the memorandum and directive which led to its creation were classified, the NSA was generally unknown to the public.").

[86] JK Davis, *Spying on America: The FBI's Domestic Counter-Intelligence Program*, U.S. Dep't Just., https://www.ojp.gov/ncjrs/virtual-library/abstracts/spying-america-fbis-domestic--counter-intelligence-program (last visited Feb. 17, 2025) ("COINTELPRO was aimed at five major social and political protest groups: The Communist party, the Socialist Workers party, the Ku Klux Klan, black nationalist hate groups, and the New Left movement. Under COINTELPRO policies, the FBI expanded its domestic surveillance programs and increasingly used questionable, even unlawful, methods in an effort to disrupt virtually the entire social and political protest process.").

[87] *See, e.g.*, Owen, *supra* note 80, at 34–35 (discussing the origins and transformation of Project MINARET).

[88] *See id.* ("Project MINARET was essentially the NSA's watch list. It used existing SIGINT accesses (to include information from Project SHAMROCK), and searched for terms, names, and references associated with certain American citizens.... [S]tarting in 1967, the NSA started

organizations active in the antiwar and civil rights movements."[89] Alongside the NSA and FBI, the CIA also had their own surveillance program. The CIA's Operation CHAOS maintained a computer index of over 300,000 people and organizations, the majority of them U.S. citizens.[90]

Project SHAMROCK, Project MINARET, Operation CHAOS, and COINTELPRO all ended in the early- to mid-1970s. By this point, these programs were likely illegal under U.S. law. In 1967, the U.S. Supreme Court decided both *Berger v. New York* and *Katz v. United States*.[91] Both cases found that wiretapping without a warrant was unconstitutional, with the *Katz* ruling providing for a "reasonable expectation of privacy" in correspondence that cannot be violated without adhering the necessary procedural safeguards (i.e., a warrant and individualized suspicion).[92] *Katz* remains good law, and under *Katz* the NSA's mass surveillance is likely unconstitutional. But it was not these cases that necessarily led to the downfall of Project SHAMROCK, Project MINARET, Operation CHAOS, and COINTELPRO.

Instead, a flurry of different events contributed to the demise of these programs: (1) a 1971 FBI break-in leaked the details of COINTELPRO; (2) the Watergate Scandal led to increased government scrutiny; (3) the Supreme Court decided *United States v. United States District Court* (*Keith Case*); and (4) the U.S. Senate's Church Committee began investigating the surveillance practices of the FBI, CIA, NSA,

---

adding selectors associated with American citizens to the watch list, establishing a 'civil disturbance' watch list.").

[89] *See id.*

[90] New York Times Archive, *'Operation Chaos'...*, N.Y. Times (June 11, 1975), https://www.nytimes.com/1975/06/11/archives/operation-chaos.html (noting that the Operation CHAOS had a computer database "containing an index of over 300,000 names and organizations, almost all of them of United States citizens and organizations unconnected with espionage").

[91] These cases overruled the previously mentioned *Olmstead* case. Berger v. New York, 388 U.S. 41 (1967); Katz v. United States, 389 U.S. 347 (1967).

[92] It is worth noting that the "reasonable expectation of privacy" test came from Judge Harlan's concurrence, not the main opinion, and therefore was not binding. However, it has since become the applicable and universally accepted standard. *Katz*, 389 U.S. at 360–62 (Harlan, J., concurring).

and Internal Revenue Services ("IRS"). The 1971 leak triggered the Church Committee investigation,[93] and the *Keith Case* held that a warrant is required for domestic surveillance.[94] However, the *Keith* court left open whether foreign intelligence surveillance requires a warrant.[95] The nail in the coffin was the Church Committees final report. The report found that these surveillance practices (specifically naming SHAMROCK, COINTELPRO, and MINARET) were civil rights abuses that had "undermined the constitutional rights of citizens."[96] This all contributed to the passing of the Foreign Intelligence Surveillance Act ("FISA") in 1978.

If FISA is considered a win for privacy rights, it was only in form, not in substance. Although FISA was posited as increasing oversight of foreign intelligence surveillance in the U.S.,[97] it had little effect on the permissible bounds of mass surveillance. FISA created the Foreign Intelligence Surveillance Court ("FISC") and requires the Department of Justice ("DOJ") to obtain a warrant from FISC before conducting

---

[93] Tom Jackman, *The FBI Break-in That Exposed J. Edgar Hoover's Misdeeds to Be Honored With Historical Marker*, Wash. Post (Sept. 1, 2021), https://www.washingtonpost.com/history/2021/09/01/fbi-burglary-hoover-cointelpro ("The revelations about COINTELPRO, a program begun by Hoover in 1956, led to congressional hearings by the Church Committee....").

[94] United States v. U.S. District Court, 407 U.S. 297, 323–24 (*Keith Case*) (1972) ("We do hold, however, that prior judicial approval is required for the type of domestic security surveillance involved in this case and that such approval may be made in accordance with such reasonable standards as the Congress may prescribe.").

[95] *Id.* at 308 ("[T]he instant case requires no judgment on the scope of the President's surveillance power with respect to the activities of foreign powers, within or without this country.").

[96] *Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities*, U.S. Senate, https://www.senate.gov/about/powers-procedures/investigations/church-committee.htm (last visited Feb. 17, 2025).

[97] *The Foreign Intelligence Surveillance Act of 1978 (FISA)*, U.S. Dep't of Just. [hereinafter *DOJ FISA*], https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1286 (last visited Feb. 17, 2025) ("Congress sought to provide judicial and congressional oversight of foreign intelligence surveillance activities while maintaining the secrecy necessary to effectively monitor national security threats."); *see also U.S. Surveillance Timeline*, *supra* note 25 ("The Foreign Intelligence Surveillance Act (FISA) sought to provide judicial and congressional oversight of foreign intelligence surveillance activities in response to the exposure of abuses of U.S. persons' privacy rights by certain components of the United States government.").

foreign intelligence surveillance.[98] FISC is a specialized court in Washington, D.C. that reviews warrant application for foreign intelligence.[99] FISC judges are picked from existing District Court Judges by the U.S. Supreme Court Chief Justice for a temporary and part time assignment.[100] In theory, this provided three branch oversight of foreign intelligence surveillance–the DOJ (executive) must request a warrant from FISC (judiciary) through the parameters set by FISA (legislature).

However, in practice, this was not the case. FISC rejected only 11 out of 34,000 warrant requests from 1979 to 2013.[101] This indicates the warrant process was more of a rubber stamp than a meaningful review. During this time the review process had a lower burden than traditional warrants, its rulings were secret (providing no congressional oversight), and adverse parties were not permitted to present evidence in it.[102] Only in 2022 did the government release a set of classified rulings from FISC, with much of it redacted.[103] Further, FISC has been criticized for serving as a rule-maker instead of its intended role as gatekeeper.[104]

---

[98] *DOJ FISA*, *supra* note 97 ("Subchapter I of FISA established procedures for the conduct of foreign intelligence surveillance and created the Foreign Intelligence Surveillance Court (FISC). The Department of Justice must apply to the FISC to obtain a warrant authorizing electronic surveillance of foreign agents.").

[99] *See generally About the Foreign Intelligence Surveillance Court*, U.S. Foreign Intel. Surveillance Ct., https://www.fisc.uscourts.gov/about-foreign-intelligence-surveillance-court (last visited Feb. 27, 2025).

[100] *Id.* ("The FISC is composed of 11 experienced federal district judges who are designated by the Chief Justice of the United States for this part-time assignment.").

[101] Schneier, *supra* note 1, at 175 (noting that FISC "rejected a mere 11 out of 34,000 warrant requests between its formation in 1979 and 2013").

[102] *See id.* at 177 ("[T]he FISA Court has a much lower standard of evidence before it issues a warrant. Its cases are secret, its rulings are secret, and no one from the other side ever presents in front of it.").

[103] *See* Matthew Guariglia & Aaron Mackey, *Victory: Government Finally Releases Secretive Court Rulings Sought By EFF*, Elec. Frontier Found. (Aug. 22, 2022), https://www.eff.org/deeplinks/2022/08/victory-government-finally-releases-secretive-court-rulings-sought-eff ("[T]he government released seven heavily-redacted but previously classified rulings from the Foreign Intelligence Surveillance Court that shed new light on how the secret court interprets key provisions of the laws that authorize mass surveillance.").

[104] *See generally* Emily Berman, *The Two Faces of the Foreign Intelligence Surveillance Court*, 91 Ind. L.J. 1191 (2016).

Essentially, while FISC *should* ensure that the government has met the necessary warrant requirements (i.e. gatekeeper), the court has instead been asked to determine whether mass surveillance is in line with existing law (i.e. rule-maker), all while operating in secret.[105]

Further, even with FISA's rubber-stamping warrant process, the court was often entirely bypassed. For example, in 2012 US Cellular received two wiretap orders approved by the judiciary.[106] That same year, the company received 10,801 subpoenas without appropriate judicial oversight.[107] Sometimes the NSA went further still, as seen in Snowden's leaks, by hacking directly into corporate infrastructure.[108] FISA failed to add meaningful safeguards against government mass surveillance, and FISA has even been weaponized against domestic citizens (even though FISA provided no justification for monitoring domestic information).[109] Further, FISA was amended in 2008 to add Section 702, which authorizes the warrantless collection of "foreign intelligence information."[110] This dismantled some of the very little protections that FISA afforded and allowed domestic citizens to be spied on if they have

---

[105] *See id.* at 1192 –93 (arguing that the FISC has become a "rule maker" post-911 as opposed to its original charge of "gatekeeper").

[106] *See* Schneier, *supra* note 1, at 177 ("US Cellular received only two judicially approved wiretap orders in 2012....").

[107] *See id.* (noting that in 2012 US Cellular additionally received "another 10,801 subpoenas for the same types of information without any judicial oversight whatsoever").

[108] *See, e.g.*, *id.* at 85 ("[N]ot satisfied with the amount of data it receives from Google and Yahoo via PRISM, the NSA hacked into the trunk connections between both companies' data centers....").

[109] *See* Berman, *supra* note 104, at 1198 ("The FISA Court has authorized at least three bulk--collection programs since 9/11, some more controversial than others. The most controversial is the bulk collection of all domestic telephony metadata....").

[110] *See Warrantless Surveillance Under Section 702 of FISA*, Am. C.L. Union, https://www.aclu.org/warrantless-surveillance-under-section-702-of-fisa (last visited Feb. 27, 2025) ("Under Section 702 of the Foreign Intelligence Surveillance Act (FISA), the U.S. government engages in mass, warrantless surveillance of Americans' and foreigners' phone calls, text messages, emails, and other electronic communications."); Noah Chauvin, *Why Congress Must Reform FISA Section 702–and How It Can*, Brennan Ctr. for Just. (Apr. 9, 2024), https://www.brennancenter.org/our-work/analysis-opinion/why-congress-must-reform-fisa-section-702-and-how--it-can ("Enacted shortly after 9/11, Section 702 allows intelligence agencies to collect the phone calls, emails, text messages, and other communications of almost any non-American located outside of the United States without a warrant.").

interactions with anyone outside of America, a practice that increased significantly in the wake of 9/11.

Returning to the chronology of U.S. mass surveillance, in 1981 President Reagan signed Executive Order 12333, which gave the government a legal basis (notwithstanding nor acknowledging *Katz*, *Berger*, or *Keith*) for this surveillance.[111] The NSA still relies on this executive order while conducting surveillance activities for foreign intelligence.[112] The executive order ambiguously permits the collection of "[i]nformation constituting foreign intelligence or counterintelligence."[113] A glimmer of hope again came from the United States Supreme Court in the 2001 *Kyllo v. United States* case.[114] In *Kyllo*, the court held that using thermal imaging to see inside someone's home without a warrant is a violation of *Katz*'s reasonable expectation of privacy and, hence, the Fourth Amendment.[115] Although it did not address foreign intelligence surveillance, it appeared to be another win for privacy rights. However, later that year, privacy rights would be all but eviscerated in the wake of 9/11.

3. Contemporary Era

Six weeks after terrorists flew three planes into the World Trade Center and Pentagon, President Bush signed into law the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 ("Patriot Act").[116] This bill was pushed to the Senate floor for a vote with "no discussion, debate, or hearings."[117] Many senators did not even have a chance to

---

[111] *Executive Order 12333*, Nat'l Sec. Agency, https://www.nsa.gov/Signals-Intelligence/EO-12333 (last visited Feb. 27, 2025) ("Executive Order (EO) 12333 is the foundational authority by which NSA collects, retains, analyzes, and disseminates foreign signals intelligence information.").

[112] *See id.*

[113] Exec. Order No. 12,333, 46 F.R. 59941 (1981).

[114] Kyllo v. United States, 533 U.S. 27 (2001).

[115] *Id.*

[116] Pub. L. No. 107-56, 115 Stat. 272 (2001).

[117] *Surveillance Under the USA/PATRIOT Act*, Am. C.L. Union (Oct. 23, 2001), https://www.aclu.org/documents/surveillance-under-usapatriot-act.

read it.[118] In the House, there was a debate, and from those debates the Judiciary Committee put forth a watered down version of the bill.[119] This compromise bill was tossed by House leadership and a bill mirroring the Senate version was moved to floor, both without debate, and the Bush administration sent a clear message: if you vote this down, the next attack will be your fault.[120]

Most relevant to mass surveillance, Section 215 of the Patriot Act permitted the FBI to force anyone (i.e. everyone) to turn over information nebulously related to "clandestine intelligence activities."[121] It was under Section 215 that tens of millions of ordinary Americans had their communications secretly recorded by the government since 2001.[122] Often, the U.S. government worked in willing cooperation with cell phone companies like AT&T.[123] In fact, "AT&T shared billions of emails and phone records from its domestic networks" with the NSA.[124] So did other companies like Verizon.[125] Overall, there was effectively nothing stopping the NSA in their surveillance. Many companies holding

---

[118] *See id.* ("Many Senators complained that they had little chance to read it, much less analyze it, before having to vote.").

[119] *See id.* ("In the House, hearings were held, and a carefully constructed compromise bill emerged from the Judiciary Committee.").

[120] *See id.* ("But then, with no debate or consultation with rank-and-file members, the House leadership threw out the compromise bill and replaced it with legislation that mirrored the Senate version.... The Bush Administration implied that members who voted against it would be blamed for any further attacks....").

[121] 50 U.S.C. § 1801(e)(1)(C).

[122] *See, e.g.*, *NSA Spying*, Elec. Frontier Found., https://www.eff.org/nsa-spying (last visited Feb. 27, 2025) ("The US government, with assistance from major telecommunications carriers including AT&T, has engaged in massive, illegal dragnet surveillance of the domestic communications and communications records of millions of ordinary Americans since at least 2001.").

[123] *See id.*

[124] Daniel Costa-Roberts, *AT&T Cooperated Extensively With NSA, Snowden Documents Reveal*, PBS News (Aug. 15, 2015), https://www.pbs.org/newshour/politics/report-att-cooperated-extensively-nsa-sharing-billions-phone-email-records.

[125] *See* Leslie Cauley, *NSA Has Massive Database of Americans' Phone Calls*, USA Today (Sept. 15, 2022), https://eu.usatoday.com/story/money/2022/09/13/nsa-secretly-collecting--americans-phone-call-records/7940563001 ("The National Security Agency has been secretly collecting the phone call records of tens of millions of Americans, using data provided by AT&T, Verizon and BellSouth....").

private citizen data willingly gave it over to the NSA. If not, the NSA would get a rubber stamp warrant from FISC (recall that only 0.03% of warrant applications were denied by FISC).[126] Occasionally this oversight was sidestepped entirely by the government hacking into corporate databases.[127] The Patriot Act had a sundown provision, but many of the bills salient provisions were permanently codified in 2005.[128]

Of course, it is likely that this surveillance went well beyond the scope of the bill. Many were shocked in 2013 when Edward Snowden, an NSA intelligence contractor, revealed the extent of this surveillance.[129] Even the author of the Patriot Act was disturbed to learn that it led to mass surveillance, contending that the bill never intended mass surveillance.[130] Among the most startling revelations were derived from the NSA's Prism and XKeyscore programs. The NSA's Prism program provided backdoor access to companies like "Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube and Apple," processing and storing vast amounts of information.[131] This allowed the NSA to log every correspondence and access those logs without a warrant.[132] Since much of the world uses American internet companies for their correspondence, Prism included vast amounts of international and domestic information.[133] It is still unclear which companies willingly complied,

---

[126] *See supra* note 101 and accompanying text.

[127] *See supra* note 108 and accompanying text.

[128] USA PATRIOT Act Improvement and Reauthorization Act, Pub. L. No. 109-177, 120 Stat. 192 (2005).

[129] *See, e.g.*, Network of Eur. Union, The NSA Leaks and Transatlantic Relations (2014) (discussing European reactions to the leaks).

[130] See *End Mass Surveillance Under the Patriot Act*, Am. C.L. Union, https://www.aclu.org/end-mass-surveillance-under-the-patriot-act (last visited Feb. 27, 2025) ("The author of the [PATRIOT Act] has publicly stated that it was never intended to facilitate mass, suspicionless surveillance.").

[131] Zoe Kleinman, *What Does Prism Tell Us About Privacy Protection?*, BBC News (June 10, 2013), https://www.bbc.com/news/technology-22839609.

[132] *See* Samuel Chapman, *Edward Snowden & the NSA PRISM Program*, Priv. J. (Nov. 21, 2024), https://www.privacyjournal.net/edward-snowden-nsa-prism ('Through the PRISM program, the NSA and other agencies can 'obtain targeted communications without having to request them from the service providers and without having to obtain individual court orders.'").

[133] *See, e.g.*, *id.* ("Because much of the world uses communication channels run by American internet firms, PRISM's back door gives U.S. intelligence direct access to a global data stream.").

which were forced to comply by court order, and which were hacked directly by the government.[134] Yahoo, for example, was threatened with a $250,000 per-day fine if they denied the NSA access.[135]

XKeyscore is potentially more intrusive than Prism. NSA described XKeyscore as its "widest reaching" data gathering mechanism.[136] XKeyscore allows for NSA agents to monitor web traffic–specifically "at least 41 billion total records" in a 30 day period–with the data being compiled to let analysts "search by name, telephone number, IP address, keywords, the language in which the Internet activity was conducted or the type of browser used."[137] However, this data is only kept for a short period of time.[138]

Even prior to these mass surveillance revelations, there were legal challenges to the statutory basis underpinning U.S. mass surveillance. A collection of people that engaged in sensitive correspondence filed a lawsuit against James Clapper, the Director of National Intelligence. Although the Supreme Court finally had the chance to declare this surveillance unconstitutional in *Clapper v. Amnesty International*, they failed to do so.[139] Instead of reaching the merits of the case, the court tossed the case due to a lack of standing, finding that the plaintiffs (which included groups that conduct sensitive and privileged correspondence such as "attorneys and human rights, labor, legal, and media

---

[134] *See id.* (noting that some telecommunications companies willingly complied, others were threatened, and the "MUSCULAR" program was focused purely on hacking directly into telecommunication infrastructure).

[135] *See, e.g.*, Kim Zetter, *Feds Threatened to Fine Yahoo $250K Daily for Not Complying With PRISM*, Wired (Sept. 11, 2014), https://www.wired.com/2014/09/feds-yahoo-fine-prism ("[T]he Feds threatened [Yahoo] the internet giant with a massive $250,000 a day fine if it didn't comply and a court ruled that Yahoo's arguments for resisting had no merit.").

[136] *See* Yannick LeJacq, *How the NSA's XKeyscore Program Works*, NBC News (Aug. 1, 2013), https://www.nbcnews.com/technolog/how-nsas-xkeyscore-program-works-6c10812168 (noting that NSA described XKeyscore as its "'widest reaching' means of gathering data from across the Internet.").

[137] *See id.*

[138] *See id.* ("Content remains on the system for only three to five days....").

[139] Clapper v. Amnesty Int'l USA, 568 U.S. 398 (2013).

organizations")[140] did not suffer any harm.[141] The standing doctrine in the United States requires that plaintiffs have: (1) an injury in fact that is (a) concrete and particularized and (b) actual or imminent; (2) a causal connection between the injury and the conduct before the court; and (3) likeliness of redressability if the court grants a favorable decision.[142] The plaintiffs in *Clapper* failed on the first prong, being unable to show they suffered an injury in fact.[143] This doctrine is convoluted and contested at best, while potentially allowing the Supreme Court to dodge meaningful questions at the worst.

Things did not go according to plan for Snowden personally. When it became public that he was the source of the leaks, he was charged with theft and violations of the 1917 Espionage Act.[144] In route to Ecuador for asylum, he landed in Moscow, where his passport was canceled.[145] He spent forty days in the Moscow airport seeking asylum but was refused at every turn.[146] Snowden eventually decided to stay in Russia, where he remains today after getting married and having two sons.[147]

On a broader level, however, there have been some minor improvements since *Amnesty International.* Two of the most important

---

[140] *Id.* at 406.

[141] *See generally id.*

[142] *See generally Standing*, Legal Info. Inst., https://www.law.cornell.edu/wex/standing (last visited Feb. 27, 2025).

[143] *Clapper*, 568 U.S. at 410 ("[R]espondents' theory of standing, which relies on a highly attenuated chain of possibilities, does not satisfy the requirement that threatened injury must be certainly impending.").

[144] *See Edward Snowden: A Timeline*, NBC News (May 26, 2014), https://www.nbcnews.com/feature/edward-snowden-interview/edward-snowden-timeline-n114871 (noting that Snowden was charged with two counts of violating the 1917 Espionage Act).

[145] *See* Dave Davies, *Edward Snowden Speaks Out: 'I Haven't And I Won't' Cooperate With Russia*, Nat'l Pub. Radio (Sept. 19, 2019), https://www.npr.org/2019/09/19/761918152/exiled--nsa-contractor-edward-snowden-i-haven-t-and-i-won-t-cooperate-with-russia (discussing the cancelation of Snowden's passport in Russia).

[146] *See id.* ("Snowden spent 40 days in the Moscow airport, trying to negotiate asylum in various countries.").

[147] *See* Greg Myre, *A Decade on, Edward Snowden Remains in Russia, Though U.S. Laws Have Changed*, Nat'l Pub. Radio (June 4, 2023), https://www.npr.org/2023/06/04/1176747650/a-decade-on-edward-snowden-remains-in-russia-though-u-s-laws-have-changed (discussing Snowden's life in Russia as of 2023).

developments came in 2015. First, the Second Circuit (a federal court just beneath the Supreme Court) ruled in *ACLU v. Clapper* that the NSA's bulk collection of data went beyond the scope of Section 215 of the Patriot Act.[148] Second, the Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act ("USA Freedom Act") was subsequently signed into law by President Obama.[149] Legislators touted that the USA Freedom Act prohibited the "bulk collection of ALL records under Section 215 of the PATRIOT Act, the FISA pen register authority, and national security letter statutes."[150] It also mandated the disclosure of certain opinions by FISC and imposed new reporting requirements for government surveillance activities.[151] However, it also made *ACLU* moot before it could reach the Supreme Court.[152]

While mass surveillance has purportedly been rolled back (by the same government that secretly did it in the first place), the fight is far from over. It is unclear if there has been meaningful change at the federal level. In 2017, the NSA stated that it had 40 surveillance targets but collected over 543 million call records.[153] Section 702 of the FISA program was recently extended past its deadline with bipartisan support.[154] It also expanded the definition of "Electronic Communications Service

---

[148] Am. C.L. Union v. Clapper, 785 F.3d 787 (2nd Cir. 2015).

[149] Pub. L. No. 114-23, 129 Stat. 268 (2015).

[150] *USA Freedom Act*, House Judiciary Comm., https://judiciary.house.gov/usa-freedom-act (last visited Feb. 27, 2025).

[151] *See generally id.*

[152] *Cf.* Clapper, 785 F.3d at 826 ("[T]he statutory issues on which we rest our decision could become moot....").

[153] *See ACLU v. ODNI – FOIA Lawsuit Seeking Records About Government Surveillance Under the USA Freedom Act*, Am. C.L. Union (Sept. 14, 2023), https://www.aclu.org/cases/aclu-v-odni-foia-lawsuit-seeking-records-about-government-surveillance-under-usa-freedom-act ("[I]n 2017, the NSA asserted it had 40 surveillance targets–and collected more than 534 million call records.").

[154] *See* The Associated Press, *Biden Signs Reauthorization of Surveillance Program Into Law Despite Privacy Concerns*, Nat'l Pub. Radio (Apr. 20, 2024), https://www.npr.org/2024/04/20/1246076114/senate-passes-reauthorization-surveillance-program-fisa ("[T]he Senate had approved the bill by a 60-34 vote hours earlier with bipartisan support, extending for two years the program known as Section 702 of the Foreign Intelligence Surveillance Act.").

Provider," to include "anyone who oversees the storage or transmission of electronic communications" such as emails, texts, or other online data, and requires them to "cooperate with the federal government's requests to hand over data."[155] Under Section 702 and Executive Order 12333, it is possible that little has changed regarding the NSA's surveillance practices today.[156]

If meaningful change is going to happen in the U.S., its best chance is derived from public sentiment. Democratically elected legislators are subject to the desires of their voters. Americans need to demand more transparency in government surveillance practices and an end to mass surveillance. The Supreme Court is unlikely to step in. In theory, a future mass surveillance challenge like *Amnesty International* could survive a standing challenge if the courts take the position that privacy violations are inherently harmful and injurious.[157] However, this is a long shot. Further, even if mass surveillance plaintiffs are given standing, U.S. courts often refuse to hear cases presenting political question, which mass surveillance and national security would likely fall under.[158] Better whistleblower protections–sufficient to encourage and protect those like Snowden–would be a great start alongside the recommendations in Part V.

B. United Kingdom

Snowden's leaks exposed considerable information about mass surveillance in the UK. In contrast to the United States, the United

---

[155] *See* Matthew Guariglia, *NSA Surveillance and Section 702 of FISA: 2024 in Review*, Elec. Frontier Found. (Dec. 28, 2024), https://www.eff.org/deeplinks/2024/11/nsa-surveillance-and-section-702-fisa-2024-year-review

[156] *See generally* Sarah Taitz, *Five Things to Know About NSA Mass Surveillance and the Coming Fight in Congress*, Am. C.L. Union (Apr. 11, 2023), https://www.aclu.org/news/national-security/five-things-to-know-about-nsa-mass-surveillance-and-the-coming-fight-in-congress.

[157] *See supra* notes 97–110 and accompanying text.

[158] *See, e.g.*, *Political Question Doctrine*, Legal Info. Inst., https://www.law.cornell.edu/wex/political_question_doctrine (last visited Feb. 27, 2025) ("Political Question doctrine is the rule that Federal courts will refuse to hear a case if they find that it presents a political question.").

Kingdom has steadily expanded its surveillance powers after the Snowden leaks. The UK now has one of the most expansive surveillance regimes in Europe, and almost certainly surpasses the U.S. in scope. Snowden, in 2016, claimed that "the US' National Security Agency could only dream of having the same power that the UK's GCHQ exercised."[159] Ironically, Britain has historically sought to avoid the centralized state power that was a French hallmark. As this paper shows, the UK consistently caught up to France's surveillance capabilities and may now claim the title for most surveilled country in Europe.

Part II.B.1 examines foreign intelligence surveillance from the late 18th century to WWI. During that time foreign intelligence surveillance played a key role in British colonialism and monitoring Irish terrorists. The lead up to WWI also saw drastic increases in UK surveillance capabilities. Part II.B.2 examines WWI to the 21st century. During this time, the UK continued to expand its intelligence capabilities, targeting both citizens and foreign diplomats. This period also gave rise to the Five Eyes Alliance. Finally, Part II.A.3 examines the contemporary framework, where it becomes apparent that the UK continues to conduct extensive surveillance domestically and internationally.

1. Pre-WWI

The UK (used interchangeably with Great Britian and its progeny) has a foreign intelligence wrinkle; their widespread colonization differentiates it from the U.S. This can be seen in Ireland–one of Britain's oldest colonies–near the turn of the 18th century. After the Irish Rebellion of 1798, the British collected statistics and census data on the Irish.[160] This surveillance paired with spies allowed the British "to control the Irish population more robustly... [and] play nationalist and

[159] Girod, *supra* note 48.

[160] *See* Eliza Egret & Tom Anderson, Mass Surveillance and Control of European Dissidence: The UK Surveillance State 4 (2021) ("Following the Irish rebellion of 1798, the British

[state] undertook mass surveillance of the Irish population, including the collection of statistics and census data.").

unionist populations off against each other."[161] A similar strategy was employed in India, where the British undertook scientific population classifications to use community and caste differences against the local population.[162] This colonial tactic would be expanded upon by the British in the Middle East after WWI, dispersing ID cards and developing "control systems such as security fences, watchtowers, permit systems and checkpoints."[163]

A domestic surveillance mechanism came from the Aliens Act of 1793.[164] This has been called Britain's "first large-scale statutory effort to control and curb immigration to the British Isles" and required immigrants to register with government officials on arrival.[165] In the early-19th century, Britain built up its police force, and from the "late 1820s-onward... engaged in unprecedented mass data collection as they sought to know and control their population[]."[166] Another early example of British surveillance came in the 1840's. In 1840 the British government made postage costs (up to a pound in weight and irrespective of distance) a penny.[167] This quintupled the volume of letters sent in Britian and solidified the governments monopoly on postage.[168] However, it was later

---

[161] *Id.*

[162] See id. at 4–5 ("After the 1858 Indian rebellion against the British East India Company, efforts

gathered apace to develop a new system of 'scientific' population classification in order to enable the famous British 'divide and rule' strategy, which consolidated British rule by weaponising the divisions between India's different religious communities and castes.").

[163] *Id.* at 5.

[164] Aliens Act 1793, 33 Geo. 3 c. 4.

[165] Jan C Jansen, *Aliens in a Revolutionary World: Refugees, Migration Control and Subjecthood in the British Atlantic, 1790s–1820s*, 255 Past & Present 189, 204 (2021).

[166] Dr. Gary Girod, *Mass Surveillance in France & Britain: The Age of the Masses*, Fr. Hist. Podcast (June 8, 2024), https://www.thefrenchhistorypodcast.com/mass-surveillance-in-france-britain-the-age-of-the-masses.

[167] *See* Editors of Encyclopaedia Britannica, *Penny Post,* Encyclopaedia Britannica https://www.britannica.com/topic/Penny-Post (last visited Feb. 27, 2025) ("All letters and packets up to one pound in weight were delivered for one penny (1 d)."); David Vincent, *Surveillance, Privacy and History*, Hist. & Pol'y, https://www.historyandpolicy.org/policy-papers/papers/surveillance-privacy-and-history (last visited Feb. 27, 2025) ("In 1840 the government slashed the cost of postage to a penny irrespective of distance, and introduced pre-payment to speed the process of delivery.").

[168] *See History: Victorian Britain*, BBC, https://www.bbc.co.uk/history/british/timeline/

revealed that British officials opened some of these letters for national security purposes.[169] This led to a national outcry, increased conversations surrounding privacy, and a stain on the British government.[170] Still, it would eventually be swept under the rug: the British government claimed that the legislature was investigating the matter, and courts avoided making decisions on this practice.[171]

In the 1880s, and as a result of Irish Fenian bombings, the London Police Department formed a counterterrorism branch. Although this branch (later named the "Special Irish Branch" and then "Special Branch") was meant to focus on Irish counterterrorism, it eventually expanded its monitoring to "anarchists and suffragists."[172] In the lead up to WWI, foreign intelligence surveillance ramped up in the UK. In 1909, because of widespread fear of Jewish and German infiltrators,[173] the British government formed the Secret Services Bureau.[174] This

victorianbritain_timeline_noflash.shtml (last visited Feb. 27, 2025) ("In the decade after the implementation of the 'penny post', the volume of letters sent in Britain increased five-fold to almost 350 million a year.").

[169] *See* Vincent, *supra* note 167 ("[A] 'paroxysm of national anger' exploded when the government was caught opening letters in the interests of national security.").

[170] *See id.* ("It was the political scandal of 1844, permanently scarring the career of the Minister and recalled at intervals down the decades until new regimes of surveillance were introduced around the time of the First World War, such as the 1911 Official Secrets Act.").

[171] *See* Bernard Keenan, *A Very Brief History of Interception*, LSE (Feb. 15, 2016), https://blogs.lse.ac.uk/medialse/2016/02/15/a-very-brief-history-of-interception/#prerogative ("The brief interception scandals of the 1840s and 1950s were dealt with by a most British method for diffusing scandal and brushing it under the carpet with minimum disruption: Parliamentary Inquiry.... Legally, the courts in England avoided making any decisions on interception powers at all.").

[172] *See* Gary Edward Girod, The Rise of the Information State: Domestic Surveillance in France and Britain During World War I at 12 –13 (2021) (Ph.D. dissertation, University of Houston).

[173] *See id.* at 14 (noting that the large Jewish community in London contributed to "[a]nti-Semitic fears of Jewish involvement in radical, international plots" and that German spy literature led to a mass fear of German invasion); *see also* Dr. Gary Girod, *Mass Surveillance in France & Britain: The Age of the Individual*, Fr. Hist. Podcast (June 15, 2024), https://www.thefrenchhistorypodcast.com/mass-surveillance-in-france-britain-the-age-of-the-individual ("Special Branch monitored suspected Jewish anarchists and some agents even learned Yiddish as they attempted to infiltrate the Jewish community.").

[174] *See* Girod, *supra* note 172, at 14 ("In response to allegations of German spying combined with the naval arms race in 1909 the British government quietly created the Secret Services Bureau, overseeing both foreign and domestic counterintelligence....").

organization was charged with counterintelligence activities and would later become the Security Service (MI5) and the Secret Intelligence Service (SIS or MI6).[175] In 1911, The Official Secrets Act was passed, authorizing investigations into people deemed "suspicious" and placing the burden of proving innocence on the accused parties.[176] That same year, it was discovered that the Special Branch was opening the letters of suffragettes after the movements' radicalization.[177]

2. WWI to 21st Century

The Secret Services Bureau was relatively small until it began to grow as a result of public fear during WWI.[178] At the end of WWI, due to intelligence being critical to the war effort, the British formed the Government Code and Cypher School ("GC&CS"), an entity focused on protecting communications and decrypting enemy communications.[179] The GC&CS was the predecessor of the Government Communications Headquarters ("GCHQ"),[180] and the GCHQ was named in Snowden's leaks as an entity conducting mass surveillance. Prior to and throughout the war there were censorship efforts and retaliation against communist and socialist sympathizers.[181] During WWI,

---

[175] *See id.* at 14 –15 n.36 (noting that branches of the Secret Serviced Bureau eventually became MI5 and MI6); Christopher Andrew, *The Establishment of the Secret Service Bureau*, Sec. Serv. MI5, https://www.mi5.gov.uk/history/mi5s-early-years/the-establishment-of-the--secret-service-bureau (last visited Feb. 28, 205) ("The Security Service (MI5) and the Secret Intelligence Service (SIS or MI6) began operations in October 1909 as a single organization, the Secret Service Bureau....").

[176] *See* Girod, *supra* note 172, at 15 ("In 1911 Parliament passed the Official Secrets Act which authorized investigations into suspicious persons. Once in court, the burden of proof was upon the accused.").

[177] *See* Girod, *supra* note 173 ("In March 1911 Special Branch covertly opened suffragettes' letters, a breach of privacy that was unthinkable just a few decades before.").

[178] *See generally id.*

[179] *Our Origins & WWI*, Gov't Commc'ns Headquarters, https://www.gchq.gov.uk/section/history/our-origins-and-wwi (last visited Feb. 28, 2025) ("Over the course of the First World War, Signals Intelligence provided valuable insight into enemy plans, so much so that a peacetime cryptanalytical unit was formed in 1919 to continue the mission. Originally called the Government Code & Cypher School, it would later be renamed GCHQ.").

[180] *See id.*

[181] *See* Girod, *supra* note 172, at 36 (discussing fears of communism towards the end of WWI).

the British implemented "broad public surveillance conducted by local police and prosecuted by civilian courts" against anti-war groups.[182] Through WWI the Secret Services Bureau had expanded its surveillance and by 1919 onwards British intelligence agencies had adopted anti--communist sentiments.[183] After WWI Britian surveilled writers that they believed were left-wing, including George Orwell.[184]

Post-WWI, the GC&CS grew and monitored foreign intelligence from countries like France, Japan, and the U.S., but primarily targeted the Soviet Union.[185] By 1939, it was most closely monitoring the German nazis. It saw considerable success during WWII, then turned its attention to the soviets during the Cold War (after having 80% of its staff cut once WWII ended).[186] The extent of GC&CS's surveillance post-WWII is still shrouded in some mystery, but it is known that they targeted a variety of countries by eavesdropping on their diplomatic conversations.[187] It is also known that WWII led to the creation of the Five Eyes Alliance ("FVEY") between the US, the UK, Canada, Australia, and New Zealand.[188] FVEY, mentioned in Snowden's leaks,

---

[182] *Id.* at 53.

[183] *See id.* at 163 ("[W]orries about the threat of communism and Bolshevism were deeply entrenched [in British surveillance agencies] by 1919.").

[184] *See generally* James Smith, British Writers and MI5 Surveillance, 1930–1960 (Cambridge Univ. Press 2013).

[185] *See* Daniel Lomas, *Beyond Bletchley: GCHQ and British Intelligence*, Hist. Today (Nov. 11, 2019), https://www.historytoday.com/archive/feature/beyond-bletchley-gchq-and-british--intelligence ("GC&CS had significant early success against French, Japanese and US communications. The main target was the Soviet Union's messages, thanks to government fears of revolution and subversion at home and in the Empire.").

[186] *See id.* ("But the emergence of the Soviet threat and the start of the Cold War would see a new peacetime organisation. By the end of 1944, there were over 10,000 staff at Bletchley and GC&CS's outstations. A year later there were just under 2,000, still far bigger than the interwar GC&CS.").

[187] *See, e.g.*, *id.* ("Beyond the main Soviet target, GCHQ also enjoyed successes against smaller foes – though much of its postwar diplomatic eavesdropping remains secret.").

[188] Scarlet Kim et al., *Newly Disclosed Documents on the Five Eyes Alliance and What They Tell Us about Intelligence-Sharing Agreements*, Yale L. Sch. (Apr. 25, 2018), https://law.yale.edu/mfia/case-disclosed/newly-disclosed-documents-five-eyes-alliance-and-what-they-tell-us--about-intelligence-sharing ("Born from spying arrangements forged during World War II, the Five Eyes alliance facilitates the sharing of signals intelligence among the U.S., the U.K., Australia, Canada and New Zealand.").

was an agreement between these English speaking countries to share all signal intelligence information and the techniques used to gather that information.[189] FVEY included the ECHELON program, which has been defined as "a global communications interception system aimed at the massive collection of electronic information."[190] Towards the end of the 20th century, during the period described as "The Troubles," British intelligence focused its surveillance on the Irish Republican Army ("IRA").[191]

3. Contemporary Era

Around the turn of the 21st century, mass surveillance of foreign intelligence would emerge from secrecy and take a more active role in British society. The Intelligence Services Act of 1994[192] codified the SIS and GCHQ and allowed for intelligence warrants.[193] This was expanded upon in the Regulation of Investigatory Powers Act of 2000 ("RIPA").[194] RIPA was the foundational legislation for much of the UK's surveillance activities. RIPA enabled covert surveillance activities and provided a defense against Article 8 of the European Convention on Human Rights ("ECHR") which, as previously mentioned, addresses privacy.[195] RIPA also provided a range of different warrants types, including for things like (1) phone calls and other correspondence,

---

[189] *See id.* ("The Five Eyes countries agree to exchange by default all signals intelligence they gather, as well as methods and techniques related to signals intelligence operations.").

[190] Lohanna Reis, *The Real History of the ECHELON Program: The "5 Eyes" Global Espionage Alliance*, Atlas Rep. (Jan. 2, 2024), https://atlas-report.com/the-real-history-of-the-echelon-program-the-5-eyes-global-espionage-alliance.

[191] *See generally* Thomas Leahy, The Intelligence War Against the IRA (Cambridge Univ. Press 2020).

[192] Intelligence Services Act 1994, c. 13 (UK).

[193] *Id.* § 5(2) ("The Secretary of State may, on an application made by the Security Service, the Intelligence Service or GCHQ, issue a warrant under this section....").

[194] Regulation of Investigatory Powers Act 2000, c. 23 (UK).

[195] Regulation of Investigatory Powers Act, Reeds City Council, https://www.leeds.gov.uk/privacy-and-data/investigatory-powers-act (last visited Feb. 28, 2025) ("RIPA provides an authorisation process for covert surveillance and information gathering, and an authorisation can be used as a defence against a claim that the council has interfered with an individual's right to private life under Article 8 of the European Convention on Human Rights.").

which require adequate justifications and a warrant from the a Secretary of State; (2) metadata access; and (3) covert surveillance warrants requiring approval from a senior officer.[196]

It was later revealed that less than 0.25% of the over three million warrants/decisions for interception requests from 2000–2010 were approved by a judge.[197] Similar to the U.S., the warrant process has been criticized as being a "rubber stamp."[198] RIPA also created the Investigatory Powers Tribunal ("IPT"), which specializes in surveillance and is akin to FISC in the U.S.[199] The IPT receives public complaints but initially held proceedings in secret, later adopting a mix of open and closed sessions.[200] The IPT has, however, appeared slightly more willingly to stand up for privacy rights, leading to two European Court of Justice decisions that were unfavorable to UK mass surveillance.[201]

After 9/11 in the United States, the UK legislature passed the Anti-terrorism, Crime and Security Act of 2001.[202] This bill, among other things, allowed for the Secretary of State to require phone and internet companies to retain data and permitted police to require individuals to

---

[196] *Investigatory Powers Act 2016: Explanatory Notes*, Legilsation.Gov.UK, https://www.legislation.gov.uk/ukpga/2016/25/notes/division/6/index.htm (providing, in Part 2, Chapters 1 and 2 the different types of warrants that can be issued under RIPA).

[197] *See* Eric Metcalfe, Justice, Freedom from Suspicion Surveillance Reform for a Digital Age 5 (2011) ("In total, there have been close to three million decisions taken by public bodies under RIPA in the last decade.... Of the decisions we do know about, fewer than 5,000 (about 0.16 per cent) were approved by a judge.").

[198] *See id*. at 106 ("This practice of authorising officers simply repeating or endorsing the application is, of course, better known as 'rubber stamping'.").

[199] *See, e.g.*, Diane P. Wood et al., *Judicial Oversight of Covert Action in the United States and United Kingdom: A Report from the 2015 United States–United Kingdom Legal Exchange*, 100 Judicature 35, 36 (2016) ("The United Kingdom's counterpart to the FISA Court, the Investigatory Powers Tribunal ('IPT')... has the power to hear complaints arising from the government's surveillance activities....").

[200] *See* Clare Feikert-Ahalt, *Foreign Intelligence Gathering Laws: United Kingdom*, Libr. of Cong. (June 2016), https://maint.loc.gov/law/help/intelligence-activities/unitedkingdom.php ("

[201] *What We Do: Open and Closed Proceedings*, Investigatory Powers Tribunal, https://investigatorypowerstribunal.org.uk/open-and-closed-proceedings (last visited Feb. 28, 2025) ("When the Tribunal was first established it sat in private. However, in 2003 the Tribunal decided that, in accordance with the principle of open justice it should, where possible, sit in public.").

[202] Anti-terrorism, Crime and Security Act 2001, c. 24 (UK).

give them identifying data (such as fingerprints).[203] After global terrorist attacks in the 2000's, CCTV cameras were erected widely across the already heavily surveilled London to keep a consistent eye on the city.[204] To this day, there are as many as 942,562 CCTV Cameras in London (one for every ten people),[205] making it one of the most surveilled cities in the world and the only top ten "surveilled city" outside of China.[206]

After the deterioration of UK privacy rights in the early 2000's, however, privacy rights in the UK seemingly had a string of victories. First, in 2008 the European Court of Human Rights held that an Electronic Test Facility ("ETF")–which intercepted up to 10,000 phone calls simultaneously between Dublin and London–violated the ECHR.[207] Then, in 2009 the House of Lords Select Committee on the Constitution published a damning report about the dangers of mass surveillance and the surveillance states' negative effects.[208] The report discussed the threats mass surveillance posed to privacy and social relationships, trust in the state, discrimination, and personal security.[209] Third, the Protection of Freedoms Act was signed in 2012,[210] which provided some protections for data and against government surveillance.

However, Snowden's 2013 leaks revealed that these victories may have had a negligible effect on the UK's surveillance systems. In particular, the leaks shed light on the GCHQ's bulk surveillance programs:

---

[203] *Id.* Part 10, 11.

[204] *See How Many CCTV Cameras Are in London?*, Clarion Sec. Sys., https://clarionuk.com/resources/how-many-cctv-cameras-are-in-london ("Research by Clarion Security Systems estimates that the amount of London Borough controlled CCTV cameras has risen from 7,911 (2012) to 20,873 (2022). An increase of 238.16% over the last 10 years").

[205] *See id.* ("Research by Clarion Security Systems estimates that there are over 942,562 CCTV Cameras in London's 607 square miles....").

[206] Matthew Keegan, *The Most Surveilled Cities in the World*, U.S. News & World Rep. (Aug. 14, 2020), https://www.usnews.com/news/cities/articles/2020-08-14/the-top-10-most-surveilled-cities-in-the-world (ranking London as the third most surveilled city, with each other country being in China).

[207] Liberty v. United Kingdom, App. No. 58243/00, Eur. Ct. H.R. (July 1, 2008).

[208] House of Lords, Select Comm. on the Const., Surveillance: Citizens and the State (2d. Sess., 2008-09).

[209] *Id.* at 99 –114.

[210] Protection of Freedoms Act 2012, c. 9 (UK).

Tempora, Karma Police, and MUSCULAR. GCHQ's project Tempora took data directly from fiber optic cables and stored vast amounts of it.[211] This included phone calls, email messages, and internet user history.[212] At its peak, the GCHQ was handling 600 million "telephone events" per day.[213] Operation Karma Police stored "billions of digital records about ordinary people's online activities" daily.[214] This effort monitored both domestic British citizens and foreign nationals.[215] Finally, the MUSCULAR program–a collaboration between the GCHQ and the NSA–bugged the telecommunications infrastructure of Google and Yahoo.[216]

The British population, however, seemed to care little about this surveillance. A poll of British citizens after the Snowden leaks found that "[o]nly 19% of British Adults say the British Security Services have too many powers."[217] Further, the same poll found that a 43% plurality

---

[211] *See* Ewen MacAskill et al., *GCHQ Taps Fibre-optic Cables for Secret Access to World's Communications*, Guardian (June 21, 2013), https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa ("One key innovation has been GCHQ's ability to tap into and store huge volumes of data drawn from fibre-optic cables for up to 30 days so that it can be sifted and analysed. That operation, codenamed Tempora, has been running for some 18 months.").

[212] *See id.* ("[Tempora] includes recordings of phone calls, the content of email messages, entries on Facebook and the history of any internet user's access to websites....").

[213] *Id.*

[214] Ryan Gallagher, *Profiled: From Radio to Porn, British Spies Track Web Users' Online Identities*, Intercept (Sept. 25, 2015), https://theintercept.com/2015/09/25/gchq-radio-porn-spies-track-web-users-online-identities.

[215] *Cf.* ("[T]he cables also transport masses of wholly domestic British emails and online chats, because when anyone in the U.K. sends an email or visits a website, that person's computer will routinely send and receive data from servers that are located overseas.").

[216] *See* Sean Gallagher, *How the NSA's Muscular Tapped Google's and Yahoo's Private Networks*, Ars Technica (Oct. 31, 2013), https://arstechnica.com/information-technology/2013/10/how-the-nsas-muscular-tapped-googles-and-yahoos-private-networks (noting that the MUSCULAR program "simply plugged into the telecommunications infrastructure that carries Google's and Yahoo's private fiber links"); *see also 10 Spy Programmes With Silly Codenames Used by GCHQ and NSA*, Amnesty Int'l (Mar. 18, 2015), https://www.amnesty.org/en/latest/campaigns/2015/03/10-spy-programmes-with-silly-codenames-used-by-gchq-and-nsa ("[MUSCULAR] intercepts user data as it passes between Google servers. Yahoo! was also said to be affected.").

[217] Will Dahlgreen, *Little Appetite for Scaling Back Surveillance*, YouGov (Oct. 13, 2013), https://yougov.co.uk/politics/articles/7546-little-appetite-scaling-back-surveillance.

felt that Snowden was aiding the "enemy" by leaking this information.[218] This provides insight into the UK legislatures next moves. In 2014, the year after the leaks, the Data Retention and Investigatory Powers Act ("DRIPA") was passed with support from the three major parties.[219] DRIPA mandates the types of data that companies must keep and requires continued cooperation with the UK government to turn communications data over under RIPA.[220]

Provisions of DRIPA were subsequently overturned by the UK courts and ultimately the European Court of Human Rights.[221] This process began with an IPT decision stating that, while mass surveillance is not allowed, the GCHQ's activities do not constitute mass surveillance.[222] The UK legislature, undeterred, enacted the Investigatory Powers Act of 2016, often referred to as "Snoopers' Charter."[223] Snowden described Snoopers' Charter as "the most extreme surveillance in the history of Western democracy."[224] On one hand, the bill required communications interception warrants to be approved by a judicial official.[225] On the other, the bill required telecommunications

---

[218] *See id.* ("Regarding the leaks themselves, 43% say they are a bad thing which aid Britain's enemies.").

[219] *See Commons Passes Emergency Data Laws Despite Criticism*, BBC (July 15, 2014), https://www.bbc.com/news/uk-28305309 ("[DRIPA is] supported by the three main parties, but opposed by civil liberties campaigners.").

[220] *See generally Data Retention and Investigatory Powers Act 2014*, UK Gov. (July 25, 2014), https://www.gov.uk/government/collectionsdata-retention-and-investigatory-powers-act-2014.

[221] R (Davis & Watson) v. Sec'y of State for the Home Dep't, [2015] EWHC (Admin) 2092 (Eng.); Sec'y of State for the Home Dep't v. Watson, Joined Cases C-203/15 and C-698/15, 2016 E.C.R. (Dec. 21, 2016).

[222] *See GCHQ Does Not Breach Human Rights, Judges Rule*, BBC (Dec. 5, 2014), https://www.bbc.com/news/uk-30345801 ("The Investigatory Powers Tribunal (IPT) says that indiscriminate trawling for information would be unlawful but the way in which the intelligence agencies go about selecting and retaining material is proportionate and lawful.").

[223] Investigatory Powers Act 2016, c. 25 (UK).

[224] Rory Cellan-Jones, *'Snoopers Law Creates Security Nightmare'*, BBC (Nov. 29, 2016), https://www.bbc.com/news/technology-38134560.

[225] *See* Home Office, Report on the Operation of the Investigatory Powers Act 2016 at 3 (2016) (noting that warrants using more intrusive powers "cannot be issued by the Secretary of State or a law enforcement chief until they have been approved by an independent Judicial Commissioner").

operators to install interception capabilities,[226] widened the scope of telecommunications operators subject to monitoring,[227] gave the Secretary of State permission to serve data retention notices to telecommunications operators (requiring them to keep data for 12 months maximum),[228] and allows for bulk warrants and bulk hacking of peoples personal devices.[229] It was around this time that Snowden claimed "the US' National Security Agency could only dream of having the same power that the UK's GCHQ exercised."[230]

Courts attempted to step in. In 2019 the UK Supreme Court ruled that IPT decisions are not immune from higher court review.[231] In 2021 the European Court of Human Rights found that the Prism and Tempora programs were too broad, did not have meaningful oversight, and harmed press freedom.[232] The 2021 decision may have come too late, as by the time that decision was handed down, the UK had already left the European Union and enacted Snoopers' Charter. In 2023, the IPT ruled that UK intelligence agencies' warrant and bulk surveillance practices were unlawful.[233] The UK government admitted to wrongdoing in the wake of

---

[226] *See* Practical Law Business Crime and Investigations, *Investigatory Powers Act 2016: Overview*, Westlaw: Practical L., https://uk.practicallaw.thomsonreuters.com/w-007-0585?transitionType=Default&contextData=(sc.Default)&firstPage=true (noting that Snoopers' Chater extended "he Secretary of State's powers to require telecommunications operators to install permanent interception capabilities").

[227] *See id.* (noting that Snoopers' Chater widened "the categories of telecommunications operators that can be subject to most powers, by including private as well as public operators").

[228] *See id.* ("Where a notice is given... [d]ata may be retained for a maximum period of 12 months.").

[229] *See People vs Snoopers' Charter: Liberty's Landmark Challenge to Mass Surveillance Powers Heard in High Court*, Nat'l Council for C.L. (June 17, 201), https://www.libertyhumanrights.org.uk/issue/people-vs-snoopers-charter-libertys-landmark-challenge-to-mass-surveillance-powers-heard-in-high-court ("[Under Snoopers' Charter] [t]hese agencies can intercept everyone's digital communications in bulk, hack into our computers, phones and tablets, and create vast 'personal datasets' without suspicion.").

[230] Girod, *supra* note 48.

[231] R (on the application of Privacy International) v. Investigatory Powers Tribunal, [2019] UKSC 22.

[232] Big Brother Watch v. United Kingdom, App. No. 58170/13 Eur. Ct. H.R. (2021).

[233] *See* David Heaton, *Investigatory Powers Tribunal Accepts Mi5 and Home Secretaries Unlawfully Issued Bulk Surveillance Warrants*, Brick Ct. Chambers (Jan. 30, 2023), https://www.brickcourt.co.uk/news/detail/investigatory-powers-tribunal-accepts-mi5-and-home-

this decision.[234] Nonetheless, the UK legislature continues to expand its mass surveillance programs. The 2023 Online Safety Act requires that social media platforms monitor all content on their platforms and make it available to UK regulators, under the banner of protecting children.[235] The 2024 Snoopers' Charter amendments require tech firms with a UK presence to notify the government of security or encryption upgrades and pause implementation pending review.[236] This is presumptively so that UK intelligence agencies can ensure continued access, while preventing companies from adapting to emerging security threats.

Contemporary mass surveillance in the UK is draconian, a violation of civil liberties under UN and EU documents, potentially unworkable, and exasperating each year. The UK government can access social media content, intercept communications with minimal oversight, and now seeks to mandate tech firms to disclose security updates–likely to ensure continued backdoor access. However, surveillance developments post-Snowden appear to have little effect on British

secretaries-unlawfully-issued-bulk-surveillance-warrants ("The Investigatory Powers Tribunal... today held that both MI5 and the Secretaries of State for the Home Department acted unlawfully over several years in relation to warrants authorising bulk interception and other bulk secret surveillance....").

[234] *See UK Government Acknowledges Past Violations of Individuals' Rights and the Fight Continues...*, Priv. Int'l (Apr. 1, 2022), https://privacyinternational.org/news-analysis/4818/uk-government-acknowledges-past-violations-individuals-rights-and-fight ("The UK government has acknowledged that section 8(4) of the Regulation of Investigatory Powers Act ('RIPA')... violated Articles 8 and 10 of the European Convention on Human Rights (ECHR).").

[235] Online Safety Act 2023, c. 50 (UK); *see also* Kevin Townsend, *UK Introduces Mass Surveillance With Online Safety Bill*, Sec. Week (Mar. 30, 2023), https://www.securityweek.com/uk-introduces-mass-surveillance-with-online-safety-bill ("To be able to determine compliance with the [Online Safety Bill], [the Government's Office of Communications] must have visibility on the content. That, in simple terms, implies mass government surveillance of any internet available to users within the UK.").

[236] Investigatory Powers (Amendment) Act 2024, c. 9 (UK); *see also* Meredith Broadbent, *A New Investigatory Powers Act in the United Kingdom Enhances Government Surveillance Powers*, Ctr. for Strategic & Int'l Stud. (May 20, 2024), https://www.csis.org/analysis/new-investigatory-powers-act-united-kingdom-enhances-government-surveillance-powers (noting that the 2024 amendments allow the UK government to "(1) force technology companies, including those based overseas, to inform the UK government of planned improvements in encryption and other enhanced security and privacy measures and (2) order a halt to such changes if the agency so chooses, pending a review, with no time limit, of the legality of the order").

public sentiment: as of 2021, a poll of UK citizens found that 58% trust British intelligence services, while less than a quarter (23%) "don't have much trust."[237]

C. France

Unlike the U.S. and UK, France was not part of the Five Eyes Alliance ("FVEY").[238] When Snowden's leaks went public, the French government expressed outrage at the purported surveillance of French citizens by the NSA.[239] The French government even required the U.S. Ambassador to France to come to Paris and explain the surveillance.[240] However, some have criticized this as a "face-saving measure" as the French government allegedly *knew* that the U.S. was spying on them.[241] Further, France was doing "the exact same thing to its own citizens" and other countries.[242] Similar to the UK, France's history of surveillance goes back centuries. Surveillance measures analogous to that of the Domesday Book (called Registers) were implemented as early as 1205 under Philip II.[243]

---

[237] Milan Dinic, *The YouGov Spying Study Part Four: Trust in UK Intelligence and Security Agencies*, YouGov (Sept. 30, 2021), https://yougov.co.uk/politics/articles/38405-part-four-trust--uk-intelligence-and-security-agenc ("One in five Britons (23%) say they don't have much trust in UK intelligence services, including 7% who say they don't trust them at all. However, 58% say they do trust the intelligence services....").

[238] However, as discussed below, France worked closely with the Five Eyes alliance.

[239] *See* Dashiell Bennett, *France Is Not Happy About the Latest Snowden Leak*, Atlantic (Oct. 21, 2013), https://www.theatlantic.com/international/archive/2013/10/france-not-happy--about-latest-snowden-leak/309770 ("A new allegation, reportedly based on leaks from Edward Snowden, claims that the NSA spied on millions of phone calls and text messages inside France. The French foreign minister calls the charge 'unacceptable'....").

[240] *See id.* ("The French foreign minister... has summoned the U.S. Ambassador to Paris, Charles Rivkin, to explain his country's actions.").

[241] *See id.* ("However, the outrage appears mainly to be a face-saving measure since French officials had to know the Americans were doing some kind of spying on them – plus, they are guilty of similar snooping as well.").

[242] *Id.*

[243] Girod, *supra* note 48 ("Philippe's new Norman administrators decided to survey his holdings in a manner similar to the Domesday Book. These are known to history as the Registers, with the first, Register A, taking place in 1205.").

Due to this, Part II.C.1 starts off with Louis XVI and the French Revolution (1787-1799), occurring contemporaneously with the founding of the U.S.[244] This period saw a continuation and exasperation of existing surveillance mechanisms, although reorientated away from the aristocracy and towards the general population. Part II.C.2 examines WWI to the 21st century, which saw the French government attempt to reel in mass surveillance efforts. Finally, Part II.C.3 examines the contemporary era. Recently, France has begun to reignite surveillance efforts and may again become a world leader in mass surveillance.

1. Pre-WWI

By 1774, French monarchs had consolidated centralized power and "Louis XVI inherited... a large bureaucracy whose royal agents surveilled the aristocracy."[245] Around this time there was considerable unrest, which cumulated in the overthrowing of the monarchy and the execution Louis XVI in 1793.[246] This gave rise to The Committee of Public Safety, whose historical reign of France was called "The Reign of Terror."[247] Maximilien de Robespierre, one of the Committee's most prominent members, established twelve member "committees of surveillance" across France, charged with monitoring and arresting those deemed suspicious.[248] As many as half a million people were targeted

---

[244] *See generally* Editors of Encyclopaedia Britannica, *French Revolution*, Encyclopaedia Britannica (Feb. 15, 2025), https://www.britannica.com/event/French-Revolution.

[245] Girod, *supra* note 172, at 4; *see also* Girod, *supra* note 48 ("France from Louis XIV to Louis XVI (r. 1774-1792) created a successful surveillance apparatus targeted against their troublesome aristocracies.").

[246] *See generally* History.com Editors, *This Day In History: King Louis XVI Executed*, Hist. (Feb. 9, 2010), https://www.history.com/this-day-in-history/king-louis-xvi-executed.

[247] *See generally* Editors of Encyclopaedia Britannica, *Committee of Public Safety*, Encyclopaedia Britannica, https://www.britannica.com/topic/Committee-of-Public-Safety (last visited Feb. 28, 2025).

[248] *See* Anthony Zurcher, *Roman Empire to the NSA: A World History of Government Spying*, BBC (Nov. 1, 2013), https://www.bbc.com/news/magazine-24749166 (noting that Maximilien Robespierre and the revolutionary government "established 12-member 'committees of surveillance' throughout the country. They were authorised to identify, monitor and arrest any suspicious former nobles, foreigners, nationals who had recently returned from abroad, suspended public officials and many more.").

by these committees.[249] During this time citizens were told they had a duty to report counter-revolutionaries.[250] Although the Committee of Public Safety would be overthrown, their successors continued to increase spies in Paris and gave sweeping authority to local military to keep the peace.[251] This shifted surveillance focuses away from the aristocracy and towards the general public, which continued when Napoleon Bonaparte effectively seized power in 1799.[252]

Napoleon developed a surveillance network that was decades ahead of the U.S. and UK and exemplified a comprehensive pre-internet surveillance society.[253] Napoleon centralized police forces by developing a hierarchical system that allowed for regular contact between localities.[254] The police would intercept communications and were required to provide reports "on [public] opinion, the press, theatres,

---

[249] *See id.* ("Historians estimate that as many as half a million people were targeted by the surveillance committees....").

[250] *See* Christopher Andrew, The Secret World: A History of Intelligence 322 (Yale Univ. Press 2018) (noting that, under the committees of surveillance, "[a]ll citizens were told they had a duty to denounce counter-revolutionaries").

[251] *See* Girod, *supra* note 172, at 4 ("In spite of Enlightenment rhetoric, the revolutionary National Assembly and its successors retained the practices of the *Ancien Régime* against anti--revolutionary threats. Already in 1789, the Assembly increased the number of police spies in Paris and adopted many of the *Ancien Régime*'s heavy-handed repressive tactics."); Girod, *supra* note 166

[252] *See* Girod, *supra* note 172, at 4 –5 ("The only major change the Revolutionary governments developed was to shift domestic surveillance from the aristocrats to the broader public."); Girod, *supra* note 166 ("[W]hile the Revolution brought down the old political order it did not greatly alter the bureaucratic apparatus nor the functions of intelligence-gathering. Its major contribution to this sector was to refocus Ancien Régime-era control mechanisms from aristocrats to the masses.").

[253] *See* Laura Kayali, *From Napoléon to Macron: How France learned to love Big Brother*, Politico (July 23, 2023), https://www.politico.eu/article/france-surveillance-cameras-privacy--security-big-brother-paris-olympics (discussing extensive surveillance efforts under Napoléon Bonaparte); Marc Fourny, *How Napoleon Monitored the French*, Le Point (July 17, 2022), https://www.lepoint.fr/histoire/comment-napoleon-surveillait-les-francais-16-07--2022-2483439_1615.php#11 (same) (translated using Google Translate); Frank Maloy Anderson, *Law for Reorganizing the Administrative System*, Napoleon Series, https://www.napoleon--series.org/research/government/legislation/c_administrative.html (last visited Feb. 28, 2025) (providing Napoleon-era legislation that helped facilitate mass surveillance).

[254] *See* Girod, *supra* note 172, at 5 ("Within three months of seizing power, Napoleon centralized police forces.... The central state established a hierarchical system and mechanisms for regular contact and supervision of localities.").

crimes, subsistence, trade, religions and emigrants."[255] This allowed Napoleon to get a consolidated view of France through networks of informants. Parisian police officers specifically were mandated to address false information and suppress misinformation (according to the states definition).[256] Napoleon also utilized the Black Chamber, or *cabinet noir*, to secretly open the mail of foreign embassies and suspected individuals.[257] However, the *cabinet noir* both preceded and lasted long after Napoleon.[258]

Napoleons police reforms lasted through the Burbon Restoration (1814-1830) and long after his reign.[259] Domestic surveillance was integrated into the Ministry of the Interior and police were continually mandated "to monitor the public mood so the state was prewarned against revolutionary outbursts."[260] France also became one of the first countries to collect national criminal statistics in 1825.[261] From the 1820's onwards France, alongside Britian, "engaged in unprecedented mass data collection as they sought to know and control their populations."[262]

However, France's shocking defeat in the 1870 Franco-Prussian

---

[255] Fourny, *supra* note 253 (translated using Google Translate); *see also* Girod, *supra* note 172, at 5 ("Minister of Police Joseph Fouché refashion the Paris police force into a well-ordered bureaucracy that monitored Parisians' views of the state.").

[256] *See* Girod, *supra* note 166 ("Uniformed police were ordered to counter false rumors and given remarkable powers to suppress what the state deemed disinformation.").

[257] *See* SpyScape, *Spy Secrets: Tales From Napoleon's Top-Secret Black Chambers*, SpyScape, https://spyscape.com/article/spy-secrets-tales-from-the-black-chambers (last visited Feb. 28, 2025) ("Codebreakers also worked alongside stenographers in the post office's secret Black Chamber, copying, deciphering, and resealing correspondence sent to foreign embassies.").

[258] *See id.* ("The *Cabinet Noir* intelligence-gathering continued as Napoleon conquered much of Europe in the early 19th century but he was not the first – or last – leader to rely on the prying eyes of the Black Chamber spies.").

[259] *See* Girod, *supra* note 166 ("While Napoleon's government maintained stability within France his foreign wars ended his empire. Yet, most of the police reforms were left in place during the Restoration.").

[260] *Id.*

[261] *See id.* ("The [French] state collected national criminal statistics starting in 1825, becoming one of the first nations to do so.").

[262] *Id.*

War exposed its intelligence shortcomings against Germany.[263] The war lasted only one year and led France to establish the *Deuxième Bureau* to conduct domestic intelligence gathering.[264] From approximately 1880 onwards the *Sûreté Générale* (originally developed by the Second Empire in the 1850's) continued to collect information on French citizens–particularly workers, Catholics, anarchists, socialists, and anti-militarists–through surveillance and attempted to shape public opinion.[265] This included the development of Carnet B in 1886, which took profiles of foreigners and subjected them to surveillance.[266]

Around the turn of the 20th century, France suffered a mass paranoia of German and Jewish spy infiltration (analogous to the British).[267] The *Section de Statistique*, part of the *Deuxième Bureau*, was at the forefront of this paranoia.[268] This period saw a multitude of accused spies being tried and convicted.[269] It also led to the Dreyfus Affair, in which the French government accused Alfred Dreyfus, an artillery officer of Jewish decent, of treason.[270] An antisemitic newspaper caught onto the story, bringing

---

[263] *See* Girod, *supra* note 173 ("The Franco-Prussian War shocked France. The country believed it was the great land power of Europe, yet Prussia and its allies defeated French armies at every turn due to their industrial and intelligence-gathering superiority which allowed for the precise movement of troops throughout eastern France.").

[264] *See id.* ("The newly-declared Third Republic recognized that France was woefully behind the new German Empire and created a series of military intelligence-gathering services. On 8 June, 1871 France inaugurated the Deuxième Bureau, which was in charge of domestic intelligence gathering." (footnote omitted)).

[265] *See id.* ("[The Sûreté Générale] collected information on all people, though primarily focused on workers and Catholic organizations.... The Sûreté's budget expanded after anarchist threats in the 1890s. Finally the gendarmerie actively engaged in surveillance, shaping public opinion and social control." (footnotes omitted)).

[266] *See id.* ("Boulanger developed the Carnet B in 1886. The Carnet B were profiles police took of foreigners.").

[267] *See id.* (discussing paranoia of German spies and rising antisemitism in the late 19th century).

[268] *See id.* ("The French military General Staff and the *Section de Statistique* inherited Boulanger's paranoia that German spies were everywhere.")

[269] *See id.* ("By 1894 a number of accused spies were convicted and even more were tried.").

[270] *See Dreyfus Affair: Topics in Chronicling America*, Libr. of Cong., https://guides.loc.gov/chronicling-america-dreyfus-affair ("French artillery officer Alfred Dreyfus, of Jewish descent, was convicted of treason in 1894 and sentenced to life in prison."); *see also* Girod, *supra* note 173 ("Lieutenant-colonel Alfred Dreyfus, an Alsatian Jew, fell victim to this paranoia when on 13 Oct. 1894 he was officially accused of treason.").

national attention and xenophobia against jews.[271] Despite strong evidence of Dreyfus's innocence, the government refused to admit its mistake, instead doubling down on the charges and even bribing witnesses against him.[272] Dreyfus was court-martialed twice, found guilty the second time, but was eventually exonerated in 1906.[273] Dreyfus's story showcases the experience that others had during this period of paranoia.

The Dreyfus Affair, and accompanying outcry, led to the *Section de Statistique* being dismantled.[274] It also led to a divide between the police and the military, as the former defended Dreyfus and the latter was his persecutor.[275] Contemporaneously, the *Sûreté Générale* kept active surveillance over anarchist and communist groups, including membership, meetings, and general activities.[276] The events of this period caused a shift in domestic intelligence gathering from the military and towards the civilian police.[277] Nonetheless, "from 1899 through WWI domestic surveillance was conducted by the *Sûreté*, *Deuxième Bureau* and local police in an overlapping web of prerogatives."[278] These different groups set the framework and infrastructure for mass surveillance through WWI and long into the future.

---

[271] *See* Girod, *supra* note 173 ("[T]he antisemitic newspaper *La Libre Parole* incensed the nation with its exposés on a traitorous Jew conspiring to destroy the French nation.").

[272] *See id.* ("The General Staff and the *Section de Statistique* did everything in its power to ensure Dreyfus' conviction rather than admit they had made a mistake which would damage their reputation.... They bribed lieutenant Eugen Lazare von Czernuski to testify against Dreyfus.").

[273] *See* Elizabeth Nix, *What Was the Dreyfus Affair?*, Hist. (June 1, 2023), https://www.history.com/news/what-was-the-dreyfus-affair (noting that Dreyfus was court martialed in 1898 and 1899, was found guilty in the 1899 trial, but was eventually exonerated in 1906).

[274] *See* Girod, *supra* note 173 ("The *Section de Statistique*'s corruption was too much for the French government. On September 12, 1899, three days after Drefyus' second conviction at Rennes, it was reorganized and stripped of its autonomy.").

[275] *See id.* ("The Affair ruptured military and police relations, as the military slandered Dreyfus and defended their prerogative while the police defended Dreyfus and the constitutional framework of the Republic.").

[276] *See* Girod, *supra* note 172, at 56 ("The *Sûreté Générale* kept an active dossier on the *Fédération Communiste Anarchiste Révolutionnaire de Langue Française*, including meeting locations, a list of its leaders, its affiliations with other radical groups, its newspapers, each chapters' year of founding, and notes on meetings and general activity.").

[277] *See* Girod, *supra* note 173 ("The [Drefyus] Affair ensured that domestic-intelligence gathering was run by civilians rather than the military.")

[278] *Id.*

During the Third Republic (1870–1940), it was also discovered that the government kept a central file of national security.[279] This file contained more than 600,000 police reports detailing political surveillance, attempts to control foreigners, and a wide variety of other things.[280] In the lead up to WWI, Paris police and the *Sûreté Générale* closely monitored labor groups and far-right groups.[281] Intelligence capabilities were expanded by the 1913 development of the Paris *Renseignements généraux de la préfecture de police* ("RGPP"), a Paris police intelligence branch and predecessor to the current *La direction du Renseignement de la préfecture de police de Paris* ("DR-PP").[282] Overall, the half-century before WWI "witnessed the emergence of agencies specialized in espionage, counterespionage, assessment, and analysis" in France.[283] These programs laid the foundation for foreign intelligence during WWI, with the war rapidly sophisticating French intelligence agencies.[284]

---

[279] *See* Kayali, *supra* note 253 ("Between 1870 and 1940, under the Third Republic, the police kept a massive file – dubbed the National Security's Central File – with information about 600,000 people, including anarchists and communists, certain foreigners, criminals, and people who requested identification documents.").

[280] *See id.*; *see also* Ministère de la Culture, *Nominative Files From the Central File of National Security (1870-1940)*, République Francaise (June 13, 2024), https://www.data.gouv.fr/fr/datasets/dossiers-nominatifs-du-fichier-central-de-la-surete-nationale-1870-1940 (Translated using Google Translate) ("The central file of the National Security... is one of the emblematic funds of the National Archives. This corpus of archives of the Ministry of the Interior is made up of more than 600,000 nominal police files from the Third Republic (1870s-1940s)....").

[281] *See* Girod, *supra* note 172, at 57–58 ("Throughout April 1914, the Paris police monitored labor groups, taking note of their meetings, speeches, organizational structure, membership and finances as they sought to measure their strength, radicalization and intentions.... Long before 1914 French intelligence services also regularly monitored far-right, antidemocratic groups.").

[282] *See generally Brief History of General Intelligence (RG)*, Direction Générale de la Sécurité Intérieure [hereinafter *France RG History*], https://www.dgsi.interieur.gouv.fr/decouvrir-dgsi/notre-histoire/breve-histoire-des-renseignements-generaux-rg (last visited Mar. 1, 2025) (Translated using Google Translate).

[283] Deborah Bauer, Marianne Is Watching: Intelligence, Counterintelligence, and the Origins of the French Surveillance State 255 (2021).

[284] *See id.* ("Intelligence agencies entered the war in a primitive, but developing, state and came out of it far more honed and professional.").

2. WWI to 21st Century

During WWI, suspected subversives to the war were closely monitored, as the French government feared again losing to the Germans in the wake of the Franco-Prussian War.[285] Internationally, France worked with Britian to establish Belgian spy networks to gather intelligence on Germany.[286] After the war, mass paranoia led to the conflation of espionage and counterespionage, leading to increased domestic surveillance efforts.[287] This period also saw a continual reorganization of intelligence efforts, particularly in the 1930s.[288] During WWII, German occupied Vichy France (1940-1944) was responsible for the "massive interception of private correspondence" to gauge public mood and watch for dissidents of the Nazi party.[289] It was also characterized by an authoritarian police state and cracking down on dissidents.[290] However, it is difficult to blame this on the French government due to the Nazi occupation.[291]

Post-WWII France gave rise to intelligence agencies focused on both domestic and international surveillance. *La direction de la surveillance du territoire* ("DST") was created in November of 1944 to operate as a domestic intelligence agency.[292] *Service de documentation*

---

[285] *See* Girod, *supra* note 172, at 60–62 (discussing extensive government control over the media and increased military strength during the start of WWI).

[286] *See* Bauer, *supra* note 283, at 257 ("The French worked in conjunction with their British allies to establish networks of observers and informers in occupied Belgium.").

[287] *See id.* at 261 (discussing French intelligence activites between WWI and WWII).

[288] *See id.* ("Throughout the 1930s the French state developed a series of branches dedicated to the collection and analysis of intelligence, for the most part tasking the army with the external collection of information and the police with domestic counterintelligence.")).

[289] Roger Austin, *Surveillance and Intelligence Under the Vichy Regime: The Service Du Controle Technique, 1939–45*, 1 Intel. & Nat'l Sec. 123, 123 (1986).

[290] *See* Lorraine Boissoneault, *Was Vichy France a Puppet Government or a Willing Nazi Collaborator?*, Smithsonian Mag. (Nov. 9, 2017), https://www.smithsonianmag.com/history/vichy-government-france-world-war-ii-willingly-collaborated-nazis-180967160 ("[A]ll the foreign Jews were put into camps, they cracked down on dissent, and it was in some ways increasingly a police state.").

[291] *Cf. id.* (noting that the Vichy France government may have been complicit in Nazi war crimes).

[292] *See France RG History*, *supra* note 282 ("In November 1944, General de Gaulle restructured the intelligence and counter-espionage services. He created the Directorate of Territorial

extérieure et de contre-espionnage ("SDECE") was created in 1946 to monitor external intelligence,[293] and was the predecessor of *Direction Générale de la Sécurité Extérieure* ("DGSE").[294] DGSE is the modern--day French analog to the NSA and GCHQ along with *Direction générale de la Sécurité intérieure* ("DGSI"),[295] which was formed in 2008.

Public outcry came in 1974 when *Le Monde* published an article that exposed the French government's Safari project, which sought to create a national computerized database of all its citizens.[296] As a result of this backlash, the *Loi Informatique et Libertés* was enacted in 1978 to better protect personal data. This act also formed the *Commission nationale de l'informatique et des libertés* ("CNIL"), which was charged with monitoring "the processing of personal data."[297] However, it is unclear how successful CNIL has been in monitoring mass surveillance, as shown by developments in the late 20th century and throughout the 21st century. One example of this is the Elysée wiretapping scandal, where it was discovered that President François Mitterrand "tapped the

---

Surveillance (DST) and confirmed the missions of the General Intelligence Service, placed within the national security.").

[293] *See From the BCRA to the DGSE*, Ministre des Armées, https://www.cheminsdememoire.gouv.fr/en/bcra-dgse (last visited Mar. 1, 2025) ("The Service de Documentation Extérieure et de Contre-Espionnage (Foreign Documentation and Counter-Espionage Service – SDECE), which came into being in 1946.... The SDECE moved to Boulevard Mortier, where it has remained ever since, only changing its name in 1982 to become the DGSE.").

[294] *See id.*

[295] *See* Nicolas Boring, *Foreign Intelligence Gathering Laws: France*, Libr. of Cong. (Dec. 2014), https://maint.loc.gov/law/help/foreign-intelligence-gathering/france.php ("It appears that large-scale communications interception is mainly done by the DGSE, which has been reported to systematically collect all telephone and electronic communications metadata in France."); *see also* Christian Chesnot, *Guilhem Giraud: "Thanks to Artificial Intelligence, Mass Surveillance Has No Limits!"*, Radio Fr. (Dec. 29, 2022), https://www.radiofrance.fr/franceculture/guilhem--giraud-grace-a-l-intelligence-artificielle-la-surveillance-de-masse-n-a-pas-de-limite-2112778 (Translated using Google Translate) (discussing mass surveillance at the DGSI).

[296] Philippe Boucher, *An IT Division is Created at the Chancellery "Safari" or the Hunt for the French*, Le Monde (Mar. 21, 1974), https://www.lemonde.fr/archives/article/1974/03/21/une-division-de-l-informatique-est-creee-a-la-chancellerie-safari-ou-la-chasse-aux--francais_3086610_1819218.html (Translated using Google Translate).

[297] Loi 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés art. 8 [Law no. 78-17 of January 6, 1978 Relating to Information Technology, Files and Freedoms].

phones of some 150 people" including politicians and journalists in the 1980s.[298] France's lack of a clear legal framework for wiretapping led to two unanimous European Court of Human Rights rulings invalidating its wiretap warrants.[299]

In response to these decisions, the French legislature tried to clarify the bounds and procedures for state surveillance. *Loi sur l'Enregistrement des Communications Électroniques* enacted in 1991 ("Wiretap Act") allowed the Prime Minister, or his designees, to approve interceptions of electronic correspondence for national security purposes.[300] It did not provide for judicial review of these decisions.[301] It did, however, establish the *Commission nationale de contrôle des interceptions de sécurité* ("CNCIS") to ensure compliance with the act.[302] CNCIS reviews authorizations made by the Prime Minister.[303] However, CNCIS decisions are not binding, and "out of 6,396 interception authorizations granted in 2011, only fifty-five received a negative recommendation by the CNCIS."[304] It is likely that oversight under the

---

[298] Jon Henley, *Bugging Scandal Lands Mitterrand Allies in Court*, Guardian (Aug. 9, 2022), https://www.theguardian.com/world/2002/aug/09/france.jonhenley.

[299] *See* Félix Tréguer, Hal Open Sci., From Deep State Illegality to Law of the Land: The Case of Internet Surveillance in France 10 (2016) ("[I]mportant criminal cases from France eventually reached the ECHR. And in two unanimous decisions issued in April 1990, the Court eventually struck down French wiretap warrants for they were not carried on 'in accordance with the law.'" (citing ECHR, Kruslin v. France, n. 11801/85, 24 April 1990; ECHR, Huvig v. France, n. 11105/84, 24 April 1990)).

[300] Loi n. 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des communications électroniques Title 2 [Law No. 91-646 of July 10, 1991 Relating to the Secrecy of Correspondence Sent by Electronic Communications] [hereinafter 1991 Wiretap Act] (authorizing the interception of foreign intelligence for national security purposes based on approval from the Prime Minister or his designates).

[301] *See generally id.*; Boring, *supra* note 295 (noting that communication interception authorizations are fully within the purview of the executive branch).

[302] 1991 Wiretap Act, *supra* note 300, at art. 13; *see also* Boring, *supra* note 295 ("The main body responsible for the oversight of interception surveillance is the Commission nationale pour les interceptions de securité (CNCIS, National Commission for Security Interceptions). When the Prime Minister (or one of his/her delegates) authorizes a communication interception, the CNCIS is to review this authorization." (footnote omitted)).

[303] *See* sources cited *id.*295

[304] Boring, *supra* note 295.

Wiretap Act has historically been weak,[305] and at the time served as the legislation underpinning France's mass surveillance activities.

3. Contemporary Era

Just prior to 9/11, in 2000, the French legislature enacted a bill requiring internet service providers "to hold and retain data that allows the identification of *any person* who has contributed to the creation of content for the services they provide."[306] Then, like the U.S. and UK, 9/11 increased mass surveillance efforts. A former DGSI engineer noted that–in the years leading up to 9/11, even with the 1990's bills–French mass surveillance was generally left to the police.[307] But after 2001 the French government began to enhance its surveillance activities.[308] In November of 2001, the French legislature amended an existing law to require telecommunications operators to retain phone and metadata.[309] While this had a sunset provision, it was later permanently codified.[310] In the 1990s France also saw the widespread implementation of video surveillance across the country.[311]

---

[305] *See id.* ("The CNCIS's recommendations do not appear to be legally binding. Parliamentary oversight appears to be weak, as requests for classified documents from parliamentary committees tend to be rejected, and members of the French Parliament have no right to hear or question members of the intelligence services.").

[306] Loi n. 2000-719 du 1er août 2000 modifiant la loi no 86-1067 du 30 septembre 1986 relative à la liberté de communication [Law No. 2000-719 of August 1, 2000 Amending Law No. 86-1067 of September 30, 1986 Relating to Freedom of Communication] (Translated using Google Translate); *see also* Tréguer, *supra* note 299, at 13–14 (translating the bill as requiring providers to retain "data allowing the identification of anybody who contributed to the creation of the content").

[307] *See* Chesnot, *supra* note 295 (noting that around 1997-1998 surveillance was a police responsibility).

[308] *See id.* ("From 2001, I noticed profound changes in doctrine, and when I returned to the DST as an engineer, I began to see this new mode of operation being put in place.").

[309] Loi n. 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne art. 29 [Law No. 2001-1062 of November 15, 2001 Relating to Daily Security]; *see* Tréguer, *supra* note 299, at 14 ("French... parliament[] amended their national law to force telecom operators to retain their users' telephone and Internet metadata." (citing *id.*)).

[310] *See* Tréguer, *supra* note 299, at 14 ("In March 2006 however, the provision was made permanent through a new vote in Parliament, though it was only in March 2006 that its implementation decree was adopted." (footnotes omitted).

[311] *See* Nteboheng Maya Mokuena, *Playing Games with Rights: A Case Against AI Surveillance at the 2024 Paris Olympics*, Geo. L. & Tech. Rev. (May 2024), https://

In 2004, amendments to the Wiretap Act replaced "telecommunications" with "electronic communications," broadening surveillance to include internet activity.[312] The 2006 attacks in Madrid and London paired with an EU 2006 data retention policy led the French legislature to enact *Loi relative à la lutte contre le terrorisme* ("2006 Terrorism Act").[313] The 2006 Terrorism Act permitted French intelligence services to access metadata retained under the 2001 bill and online content under the 2000 bill.[314] Intended solely for counterterrorism, the law included a sunset provision but was repeatedly extended.[315]

In 2008, France faced another scandal when details of EDVIGE, a sweeping government surveillance database, was leaked.[316] It was just a couple years later in 2011 when France signed the Lustre agreement with the Five Eyes Alliance ("FVEY").[317] The Lustre agreement was an international cooperation agreement that shared mass surveillance

georgetownlawtechreview.org/playing-games-with-rights-a-case-against-ai-surveillance-at-the--2024-paris-olympics ("[I]n the 1990s, France implemented widespread video surveillance across the country to reduce police response time and petty crime.").

[312] *See* Tréguer, *supra* note 299, at 17 ("[T]he Wiretapping Act was also quietly amended in 2004.... This legislative patch changed the word 'telecommunications' for 'electronic communications,' which was deemed enough to extend the Act's scope to Internet communications." (citing Loi n. 2004-669 du 9 juillet 2004 relative aux communications électroniques et aux services de communication audiovisuelle [Law No. 2004-669 of July 9, 2004 Relating to Electronic Communications and Audiovisual Communication Services])).

[313] Loi n. 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers [Law No. 2006-64 of January 23, 2006 Relating to the Fight Against Terrorism and Containing Various Provisions Relating to Security and Border Controls].

[314] *See* Tréguer, *supra* note 299, at 14 –15 (discussing the type of data that the 2006 bill authorized intelligence agencies to access).

[315] *See id.* at 15 ("Also introduced as a sunset provision, administrative metadata access was prolonged a first time in December 2008 and then again in December 2012, despite criticisms from the French Human Rights League.").

[316] *See* Julian Sanchez, *Big Sister is Watching: EDVIGE and the Angry French*, Ars Technica (Sept. 9, 2008), https://arstechnica.com/tech-policy/2008/09/big-sister-is-watching-edvige--and-the-angry-french ("The new database, known as EDVIGE, has sparked a firestorm of opposition from French unions, non-profits, and civil liberties groups since the national privacy watchdog, CNIL, forced the government to make its existence public in July.").

[317] *See generally* Jacques Follorou, *Surveillance: DGSE Transmitted Data to the American NSA*, Le Monde (Oct. 30, 2013), https://www.lemonde.fr/international/article/2013/10/30/surveillance-la-dgse-a-transmis-des-donnees-a-la-nsa-americaine_3505266_3210.html (Translated using Google translate).

intelligence between France and FVEY.[318] The Lustre agreement led DGSE to transmit "millions of data relating to the private lives of millions of French people" to the NSA, with little apparent oversight from CNCIS.[319]

It is interesting to note that Snowden's 2013 leaks did not lead to a strong backlash in France.[320] Later that year, the muted public response enabled the French legislature to further erode privacy rights. *Loi de programmation militaire 2014-2019* ("Military Bill 2013"),[321] which faced strong opposition,[322] gave government surveillance agencies real time access to metadata.[323] The following year, amid the rise of ISIS, a new law was passed that circumvented warrant requirements and gave additional powers to law enforcement and intelligence agencies.[324] These terrorism fears were realized in January 2015 when terrorists attacked Charlie Hebdo, a French satirical magazine, for their depictions of Islam.[325] This contributed to the passing of France's first comprehensive surveillance law, the *Loi relative au renseignement*

---

[318] *See id.* (noting that the Snowden leaks revealed "the existence of a cooperation agreement on surveillance between France and the United States known as 'Lustre'".).

[319] *Id.*

[320] *See* Tréguer, *supra* note 299, at 23 ("[T]he French civil society reaction to the Snowden disclosure –the first of which appeared in Guardian article on June 5th, 2013– was relatively mild.").

[321] Loi n. 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale [Law No. 2013-1168 of December 18, 2013 Relating to Military Programming for the Years 2014 to 2019 and Containing Various Provisions Concerning Defense and National Security].

[322] *See* Tréguer, *supra* note 299, at 31 (noting that the Military Bill 2013 has "growing mobilization by civil society, media attention to the issue, and increasingly vocal opposition by a few MPs....").

[323] *See* source cited *supra* note 321; Tréguer, *supra* note 299, at 29 ("[T]he government's proposal provided intelligence agencies with both ex post and real-time access to metadata, including geographic metadata.").

[324] *See* Tréguer, *supra* note 299, at 34 ("[A]nother [bill] was introduced in great fanfare in July 2014. The law greatly reinforced the power of intelligence and police agencies by circumventing traditional criminal procedures." (citing Loi n. 2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme [Law No. 2014-1353 of November 13, 2014 Strengthening the Provisions Relating to the Fight Against Terrorism])).

[325] *See generally* John Leicester, *The Charlie Hebdo Slaughter and Follow-up Terror Attacks 10 Years Ago That Changed France*, Assoc. Press (Jan. 7, 2025), https://apnews.com/article/france-charlie-hebdo-photos-terror-f42dc6d41b376ce2f7abec0e75760e7e.

("Intelligence Act").[326] Unlike the U.S. post-9/11 Patriot Act, however, the Intelligence Act may have been long in the making.[327] Terrorism fears were again exasperated on November 13, 2015, when terrorists attacked Paris, killing at least 130 and injuring 350.[328]

The Intelligence Act expanded permissible intelligence-gathering techniques, broadened surveillance justifications, permitted the French government to increase the amount of agencies with surveillance capabilities, and provided penalties (including imprisonment) for companies failing to comply with surveillance measures or data requests.[329] It also developed a new commission to replace the CNCIS, the *Commission nationale de contrôle des techniques de renseignement* ("CNCTR").[330] Like the CNCIS, the CNTCR only issues non-binding opinions on surveillance requests, and the Intelligence Act did not provide for judicial oversight.[331] Moreover, CNTCR lacks oversight of data-sharing with international foreign intelligence agencies, creating a significant loophole.[332]

The Intelligence Act also permitted the installation of black boxes in telecommunication and internet service provider infrastructure to monitor and collect real-time web traffic.[333] The Intelligence Act

---

[326] *Cf.* Boring, *supra* note 295 ("Although the adoption of the Law was probably accelerated by the intensity of the threat of terrorism and, in particular, the January 2015 attacks in France, the government emphasized that it was the result of thorough reflection and not enacted under the pressure of any specific urgent situation.").

[327] *See id.*

[328] *See generally* Michael Ray, *Paris Attacks of 2015*, Encyclopedia Britannica (Feb. 14, 2025), https://www.britannica.com/event/Paris-attacks-of-2015.

[329] *See* Tréguer, *supra* note 299, at 38 –39 (discussing general provisions of the Intelligence Act).

[330] *See id.* at 39 (discussing the CNCTR and surveillance oversight under the Intelligence Act).

[331] *See id.* at 39 –40 (same).

[332] *See id.* at 40 ("One hugely significant exception to the CNCTR's oversight powers are [the] bulk of data obtained through data-sharing with foreign intelligence agencies." (citation omitted)).

[333] *See id.* at 40 –41 (discussing black boxes under the Intelligence Act); *see also France: New Surveillance Law a Major Blow to Human Rights*, Amnesty Int'l (July 24, 2015), https://www.amnesty.org/en/latest/news/2015/07/france-new-surveillance-law-a-major-blow-to-human-rights ("[The Intelligence Act] allows the use of mass surveillance tools that capture mobile phone calls and black boxes (for the purposes of counterterrorism) in internet service providers that collect and analyse the personal data of millions of internet users.")

further authorized the hacking of computer systems, explicitly legalized the DGSE's international surveillance, and imposed data retention requirements for government intelligence agencies, among other provisions.[334] Later, in 2023, the French legislature adopted a bill permitting "law enforcement agents to remotely tap into the cameras, microphones and location services of phones and other internet-connected devices of some suspected criminals."[335]

There have been judicial challenges against this surveillance. In a Constitutional Court challenge to the Intelligence Act, it was generally upheld, but some provisions were declared invalid including Article 854-1 (which addressed international surveillance) and parts of Article 821-6 (which addressed real-time monitoring through devices).[336] In 2020 the Court of Justice of the European Union mandated that EU law applies to member states forcing telecommunications operators to retain data.[337] In 2021 the *Conseil d'État* referred the legality of mandated data retention measures in France to the Court of Justice of the European Union.[338] In 2024 the EU Court of Justice ruled on this by reemphasizing that access to personal data must meet the proportionality requirement in Article 15(1) of Directive 2002/58.[339] It is worth noting that, unlike the U.S. and UK, France operates on a Civil Law system that does not have binding judicial precedents.[340]

---

[334] *See* Tréguer, *supra* note 299, at 41–44.

[335] Youcef Bounab, L*awmakers Approve Bill Allowing French Police to Locate Suspects by Tapping Their Devices*, PBS News (July 18, 2023), https://www.pbs.org/newshour/world/lawmakers-approve-bill-allowing-french-police-to-locate-suspects-by-tapping-their-devices.

[336] Conseil constitutionnel [CC] [Constitutional Court] decision No. 2015-713 DC, July 23, 2015, https://www.conseil-constitutionnel.fr/decision/2015/2015713DC.htm.

[337] *See LQDN, FDN and Others v. France*, Priv. Int'l, https://privacyinternational.org/legal-action/lqdn-fdn-and-others-v-france (last visited Mar. 1, 2025) ("EU law applies every time a national government forces telecommunications providers to process data, including when it is done for the purposes of national security.").

[338] Conseil d'État, Assemblée, 21/04/2021, 393099 [Council of State, Assembly, 04/21/2021, 393099].

[339] 2024 E.C.J. Case C-470/21, La Quadrature du Net and Others.

[340] *See, e.g.*, *The Layout of the French Legal System*, Geo. L. Libr. (Nov. 11, 2024), https://guides.ll.georgetown.edu/francelegalresearch/legalsystem ("France is a civil law system which means it places a greater emphasis on statutes as found within various codes, instead of case law.").

From the Age of Aristocracy through Napoleon, the French outpaced the U.S. and UK in their surveillance efforts. Then, arguably, from the late 19th century through to the 21st century France's mass surveillance efforts fell behind. Now, they may have moved back into the forefront (based on public knowledge of government surveillance activities), partially as a result of the 2024 Paris Olympics. *Loi olympiques et paralympiques* ("Olympics Law")[341] was passed in May 2023 in the midst of civil rights campaigns against it.[342] The Olympics Law allowed, for the first time in Europe, AI-powered mass video surveillance.[343] Under the Olympics Law AI analyzes real-time footage to make determinations about suspicious activity.[344] This measure also led to hundreds of cameras being added to the already heavily-surveilled Paris.[345] This AI facial recognition bill had a sundown provision for December 2024, but was already extended until March 2025,[346] and police members have advocated for its extension or permanent codification.[347]

---

[341] Loi n. 2023-380 du 19 mai 2023 relative aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions [Law No. 2023-380 of May 19, 2023 Relating to the 2024 Olympic and Paralympic Games and Containing Various Other Provisions].

[342] *See generally* Laura Kayali, *French Surveillance System for Olympics Moves Forward, Despite Civil Rights Campaign*, Politico (Mar. 8, 2023), https://www.politico.eu/article/paris-olympics-surveillance-arsenal-moves-ahead-despite-civil-rights-campaign; *France: Allowing Mass Surveillance at Olympics Undermines EU Efforts to Regulate AI*, Amnesty Int'l (March 23, 2023), https://www.amnesty.org/en/latest/news/2023/03/france-allowing-mass-surveillance-at-olympics-undermines-eu-efforts-to-regulate-ai.

[343] *See 'All-out Assault on Privacy': France is First EU Country to Legalise AI-driven Surveillance*, Brussels Times (Mar. 29, 2023), https://www.brusselstimes.com/430820/all-out-assault-on-privacy-france-is-first-eu-country-to-legalise-ai-driven-surveillance ("This is the first time algorithmic mass surveillance is authorised in Europe....").

[344] *See id.* ("AI-driven surveillance analyses footage in real-time, scans and captures data from all people within its radius, and makes predictions and determinations about them.").

[345] *See* Alberto Senante, *Paris Olympics Security: Unprecedented AI Surveillance Creates Another Risk*, WorldCrunch (July 26, 2024), https://worldcrunch.com/culture-society/paris-olympics-security-surveillance ("More than 400 cameras will be added to the 4,000 already operating in Paris and placed at the entrances to stadiums, streets and nearby transport....").

[346] *See* David Coffey, *Privacy Fears Grow as France Extends Ai Surveillance Beyond Olympics*, RFI (Nov. 11, 2024), https://www.rfi.fr/en/france/20241011-privacy-fears-grow-as-france-extends-ai-surveillance-beyond-olympics-avs (noting that France extended "AI-powered video surveillance in public spaces until March 2025").

[347] *See id.* ("Paris Police Chief Nunes has backed the system, calling it necessary for public safety.").

This potentially conflicts with the EU Artificial Intelligence Act ("EU AI Act") and GDPR.[348] The EU AI Act banned biometric categorizations and the development of facial recognition databases.[349] There is a law enforcement carve-out in public spaces, but the carve-out is limited to narrow situations targeting specific individuals under specific circumstances.[350] The Olympics Law also may run afoul of EU court precedents banning mass surveillance.[351] Outside of the legal considerations, AI facial recognition efforts in the U.S. have already led to racial disparities in accuracy and enforcement.[352] However, the European Court on Human Rights tossed a challenge to French surveillance programs in January of 2025.[353] It remains to be seen whether this AI driven surveillance will be extended yet again.

III. JURISDICTIONAL COMPARISON

Overall, in recent history each jurisdiction has implemented wide-spread mass surveillance practices in the name of national security. The U.S., UK, and France took different paths to arrive at this point. Prior to the 20th century, France's surveillance practices were considerably

---

[348] *See* Mokuena, *supra* note 311 (noting that the surveillance may violate the GDPR due to processing mass biometric data).

[349] Press Release, Artificial Intelligence Act: MEPs Adopt Landmark Law, (Mar. 13, 2024), https://www.europarl.europa.eu/news/en/press-room/20240308IPR19015/artificial-intelligence-act-meps-adopt-landmark-law ("The new rules ban certain AI applications that threaten citizens' rights, including biometric categorisation systems based on sensitive characteristics and untargeted scraping of facial images from the internet or CCTV footage to create facial recognition databases.").

[350] Artificial Intelligence Act (Regulation (EU) 2024/1689) art. 5(1)(h).

[351] A list of such cases can be found at Press Unit, Eur. Ct. Hum. Rts., Mass Surveillance: Fact Sheet (2024), https://www.echr.coe.int/documents/d/echr/fs_mass_surveillance_eng.

[352] *See* Kashmir Hill, You Face Belongs to Us (2023) (noting that, when AI facial recognition used by law enforcement identified the wrong person, "[i]n every case, the man wrongfully arrested was black").

[353] *See generally* Press Release, Eur. Ct. Hum. Rts., Court Declares Inadmissible Applications by Journalists and Lawyers Concerning Convention Compatibility of French Intelligence-Gathering Legislation (Jan. 16, 2025) (available at HUDOC).

more comprehensive than either the U.S. or UK. France has a long tradition of collecting data and closely monitoring its citizens.[354] Surveillance author Olivier Aïm adopted this position, noting: "Historically, France has been at the forefront of these issues, in terms of police files and records."[355] Britian was often not far behind. Dr. Gary Girod, an expert in World War I domestic intelligence, explains that "[a]rguably since the Middle Ages, England, then Britain followed a pattern with regards to French social control mechanisms: first they sneered, then they copied."[356] However, France (as far as we know) fell behind the U.S. and UK through the 20th century until recently catching up with the Intelligence Act and Olympics Law.

The chronology of surveillance practices also sheds light on how mass surveillance mechanisms develop. Often war or civil unrest is the catalyst for the development of surveillance infrastructure. In the U.S., this came in the form of the Civil War, WWI, First Red Scare, WWII, Second Red Scare, Civil Rights Movement, and 9/11. In the UK, it was colonial unrest, Irish Fenian bombings, pre-WWI mass hysteria, WWI, WWII, 9/11, and the 2005 London Bombings. In France, it was the French Revolution, Napoleon's reign, the 1870 Franco-Prussian War loss, pre-WWI mass hysteria, WWI, WWII, 9/11, and terrorist attacks in the 2010's. However, it is worth noting that even before the French Revolution there was existing surveillance infrastructure in France. The correlation between these periods of uncertainty and increased surveillance echoes a point made earlier in the paper: people are more willing to give up civil liberties when they are afraid.[357]

Contemporary mass surveillance appears to be faltering in the U.S. but exasperating in the UK and France. The USA Freedom Act in 2015 sought to rein in mass surveillance practices, and there has been little

---

[354] See Kayali, *supra* note 253 ("[France's] tradition of snooping, monitoring and data collection dates way back....").

[355] *Id.*

[356] Girod, *supra* note 173.

[357] *See generally* Sunstein, *supra* note 21.

public development since then. In the UK, the 2016 Snoopers' Charter, 2023 Online Safety Act, 2024 Snoopers' Charter amendments, and extensive CCTV surveillance of London all appear to be going in the other direction. In France, the 2015 Intelligence Act and 2023 Olympics Law similarly increased mass surveillance. Part of this is likely due to public sentiments on mass surveillance programs. As previously mentioned, contemporary Americans tend to be extremely averse to mass surveillance,[358] while British people are much more open to it.[359] Polling of French citizens on the matter does not appear to be readily available, but French civil rights groups have constantly opposed surveillance legislation. It remains to be seen what effect EU precedents and law have on French surveillance practices, but it appears to have done little thus far.

In each of these three jurisdictions, their respective judiciaries have had an insignificant effect on these practices. The U.S. Supreme Court has several lines of cases addressing privacy rights,[360] but has not addressed the parameters governing, or the legality of, mass surveillance. UK courts have been more willing to step in, but the UK legislature continues to increase surveillance mechanisms. EU courts have similarly been critical of the UK's surveillance practices, but to little effect. This is especially true given the UK's decision to leave the EU. In France, courts have cautiously attempted to set the outer bounds of this surveillance with help from EU courts, but it is difficult to say that this has led to decreased surveillance activities. Also, France has seen less strategic litigation related to surveillance practices and has less mechanisms to receive government information.[361] While U.S. citizens can

---

[358] *See supra* notes 43–45 and accompanying text.

[359] *See supra* note 237 and accompanying text.

[360] *Katz v. United States* and its progeny provide for a "reasonable expectation of privacy." There was another string of cases protecting abortion and contraceptives through a "penumbras" of privacy rights in the constitution, but that line of cases has since been overturned. *See* Dobbs v. Jackson Women's Health Organization, 597 U.S. 215 (2022).

[361] *See* Tréguer, *supra* note 299, at 26 ("[R]egarding strategic litigation, itis worth noting that in the French legal system, legal opportunities had been lacking.").

place Freedom of Information Act ("FOIA") requests, the French equivalent "has extremely broad national security exemptions and is generally much weaker."[362]

Lastly, it is important to note a limitation in the chronology of surveillance practices and the accompanying comparison. Historically and inherently surveillance practices have been secretive. Surveillance is effective *precisely because* foreign intelligence can be intercepted without the sender or recipient being aware that the data may be compromised. As such, countries often seek to keep their surveillance outside of the public eye. This means that, often, public knowledge is limited to information that has either been leaked or declassified. Declassification often comes after a considerable amount of time has passed (if it is declassified at all) and does little to inform the public's understanding of contemporary surveillance. The programs included in Snowden's leaks may still continue outside of the public's eye. Or maybe they were replaced by newer and more intrusive programs. Even if the government unequivocally tells its citizens that surveillance has been rolled back, or that they are transparent about current practices, history has shown that it may not be the case.

IV. BALANCING NATIONAL SECURITY AND CIVIL LIBERTIES

The negative impacts of mass surveillance on privacy and civil liberties has already been delineated, but a few more points deserve attention.[363] Mass surveillance has often been weaponized against marginalized groups, protestors, and migrants.[364] Fiscally it has proven

[362] *Id.*

[363] *See supra* Part I.

[364] *See Costs of War: Surveillance*, Brown Univ.: Watson Inst. for Int'l & Pub. Affs. (Sept. 2023), https://watson.brown.edu/costsofwar/costs/social/rights/surveillance ("Mass surveillance has intensified the criminalization of marginalized and racialized groups, from Muslims and Arabs to Latinx immigrant communities to Black and Indigenous organizers, and has

expensive. For example, in 2023 the U.S. allocated $99.6 billion to intelligence.[365] From 2015 to 2019, one NSA program cost taxpayers $100 million and provided no tangible security benefits.[366] The legal grey areas that these agencies have operated in provide little meaningful oversight from legislators, the judiciary, or the general public. Mass surveillance and logging recorded information also threatens the security of that data. Intelligence agencies backdooring or black boxing into telecommunications and social media platforms exposes (and potentially creates) weaknesses that others can exploit.[367] The UK's 2024 Snoopers' Charter amendments go a step further, allowing the government to block security updates. Government's storing data also provides hackers with another potential avenue to access that data and use it for insidious goals such as blackmail.

Yet, the pertinent question remains: does mass surveillance keep us safe? Safety, or at least the appearance of safety, has justified mass surveillance on the grounds of national security. It is also the reason that British people still strongly support surveillance activities. However, there is evidence that mass surveillance actually hinders national security. The Council of Europe Parliamentary Assembly, after the Snowden leaks, cited several studies concluding that "mass surveillance does not appear to have contributed to the prevention of terrorist attacks."[368] This

---

increasingly targeted protest movements such as Black Lives Matter and the movement to stop the Dakota Access Pipeline.").

[365] *See* Michael E. DeVine, Cong. Rsch. Serv., R44381, Intelligence Community Spending Trends (2024) ("For FY2023, Congress appropriated a total of $99.6 billion [for intelligence].") The report also indicates there may be considerable spending that is not publicly available.

[366] *See* Conor Friedersdorf, *The Costs of Spying*, Atlantic (Feb. 28, 2020), https://www.theatlantic.com/ideas/archive/2020/02/costs-spying/607177 ("A new study reveals that from 2015 to 2019, the NSA's call-metadata program cost taxpayers $100 million and provided practically no useful information.").

[367] U.N. GAOR, 51st Sess., U.N. Doc. A/HRC/51/17 at 4 (Aug. 4, 2022) ("[H]acking relies on and exploits the existence of security flaws in computer systems. By keeping such vulnerabilities open, or even creating them, those resorting to hacking may contribute to security and privacy threats for millions of users and the broader digital information ecosystem.").

[368] Council of Eur., Parliamentary Assembly, Comm. on Legal Affs. & Hum. Rts., Mass Surveillance 2 (2015).

report also noted that mass surveillance programs used extensive resources that could have been used to successfully prevent attacks, but were instead diverted to ineffective mass surveillance programs.[369] Independent reviews conducted by U.S government agencies came to the same conclusion: mass surveillance has not made us any safer.[370] Instead, legitimate signs of danger have been lost amongst massive amounts of irrelevant data about millions of citizens worldwide.[371] These reports led to the startling conclusion that "the government's mass surveillance programs operating under Section 215 of the Patriot Act have *never* stopped an act of terrorism."[372] It is important to note that further research into mass surveillance's effectiveness is somewhat limited by the lack of publicly available information.

None of this is to say that foreign intelligence surveillance should be abandoned completely. Foreign intelligence surveillance remains a national defense necessity. This is evident as foreign intelligence has enabled the U.S., UK, and France to thwart terrorist attacks in recent years.[373] However, the surveillance practices of these three countries all

---

[369] *Id.* ("[R]esources that might prevent attacks are diverted to mass surveillance, leaving potentially dangerous persons free to act.").

[370] *See* Elizabeth Goitein, *Rolling Back the Post-9/11 Surveillance State*, Brennan Ctr. for Just. (Aug. 25, 2021), https://www.brennancenter.org/our-work/analysis-opinion/rolling-back-post-911-surveillance-state ("Two independent reviews found that [NSA's bulk collection] program yielded little-to-no counterterrorism benefit.

[371] *See id.* ("[T]here is evidence that overcollection is counterproductive. Multiple government reviews of domestic terrorist incidents have found that agents missed signs of trouble because those signs were lost in the noise of irrelevant data.").

[372] Rachel Nusbaum, *Ignore the Drumbeat of Doom, the NSA's Call Records Program Didn't Stop a Single Terrorist Attack*, Am. C.L. Union (Mar. 4, 2015), https://www.aclu.org/news/national-security/ignore-drumbeat-doom-nsas-call-records-program-didnt-stop-single-terrorist-attack (emphasis added); *see also* Cindy Cohn & Dia Kayyali, *The Top 5 Claims That Defenders of the NSA Have to Stop Making to Remain Credible*, Elec. Frontier Found. (June 2, 2014), https://www.eff.org/deeplinks/2014/06/top-5-claims-defenders-nsa-have-stop-making-remain-credible ("[T]op NSA official John Inglis admitted that the phone records program has not stopped any terrorist attacks aimed at the US....").

[373] *See generally FISA Section 702 Value*, Intel.gov (Feb. 14, 2024), https://www.intel.gov/assets/documents/702%20Documents/FISA_Section_702_Vignettes-20240214_Final.pdf; *see also* Sec'y of State for the Home Dep't, The United Kingdom's Strategy for Countering Terrorism 8 (2018) ("Since last year's Westminster attack, the police and the security and intelligence agencies have successfully foiled a further 12 Islamist plots, and since 2017, have

suffer from flaws related to *proportionality* and *transparency*. The *proportionality* flaw is that these mass surveillance programs are analogous to "scooping up the entire ocean to guarantee you catch a fish."[374] Not only is it impractical, but the time and effort required to implement and monitor these systems diverts resources away from targeted efforts with higher success rates. This ensures that crucial leads, which could prevent attacks, are likely to be missed.

The *transparency* flaw is that these mass surveillance programs have little effective oversight. This allows these foreign intelligence programs to be weaponized against non-foreign actors that do not pose threats to the population (civil rights groups, labor unions, political parties, etc.). Further, it has perpetuated the risk of civil rights abuses against already marginalized groups. These programs that have operated primarily in secret often provide little recourse for errors, and often the victims of those mistakes never get their day in court. Since the implementation of mass surveillance regimes has been ineffective (from a national security standpoint) and harmful (from a privacy and civil liberties standpoint), yet foreign intelligence remains a critical aspect of national security, these programs need to be restructured into a framework that seeks to maximize the benefits while minimizing the drawbacks. The next section provides guidance on how that can be done.

V. RECONCILIATION & THE PATH FORWARD

Throughout the years, mass surveillance has continually taken different forms and has been informed by different rationales. However,

disrupted four extreme right-wing plots."); *see also, e.g.*, Kim Willsher, *French Minister Warns of 'Threat From Within' on Charlie Hebdo Attack Anniversary,* Guardian (Jan. 7, 2025), https://www.theguardian.com/world/2025/jan/07/social-media-fuelling-rising-terror-threat-in-france-says-minister ("Bruno Retailleau said French intelligence had foiled nine planned attacks last year....").

[374] Schneier, *supra* note 1, at 174.

the throughline for all of histories surveillance practices is that innocent people, generally those from marginalized groups, unnecessarily suffer. Surveillance practices and mass hysteria hurt people like Dreyfus and Dr. Ibrahim. Their stories are the ones that we know about – many more have suffered from these policies, but their stories were never told. Dreyfus and Dr. Ibrahim were also vindicated in the end, while countless suffered and were never granted respite. Often, this suffering has been chalked up to a "necessary evil" in order to protect national security.

However, as this paper shows, mass surveillance is ineffective at best and at worst actively hinders national security efforts. Mass surveillance is time consuming and resource intensive, and there is little evidence that it is money and time well spent. Even if AI is integrated into mass surveillance technology, it cannot serve as a substitute for human judgement, and risks perpetuating racism and stereotypes that could further harm marginalized communities.[375] Overall, there is no place in contemporary society for mass surveillance as it was presented in Snowden's leaks. However, this paper proposes four reforms that can maximize the benefits of foreign intelligence surveillance while mitigating the drawbacks.

A. Meaningful Surveillance Oversight

The first proposal is for the development of meaningful oversight throughout the intelligence surveillance process. There should be three branch oversight of intelligence surveillance activities. This was *de jure* enacted through FISA in the U.S. and Snoopers' Charter in the UK but was not followed closely. The legislature should require warrants for surveillance and outline the applicable standards for these warrants.

---

[375] *See* Rachel Fergus, *Biased Technology: The Automated Discrimination of Facial Recognition*, Am. C.L. Union: Minn. (Feb. 29, 2024), https://www.aclu-mn.org/en/news/biased-technology-automated-discrimination-facial-recognition ("Studies show that facial recognition is least reliable for people of color, women, and nonbinary individuals. And that can be life-threatening when the technology is in the hands of law enforcement.").

These standards should require individualized and reasonable suspicion. Surveillance legislation should also provide strict regulations on the scope and duration of data retention. This would include ensuring that collected data is securely stored and should seek to limit mass transfers of data to international governments. There should also be additional whistleblower protections for people that expose government surveillance malfeasance like Edward Snowden. Further, surveillance legislation should have sundown provisions and be subject to continual reviews by the legislature.

The judicial branch should receive warrant requests and make determinations based on the guidelines set by the legislature and, if applicable, case law precedent. This should be a meaningful review, not the rubber stamp process we have seen from FISC. Further, these rulings should be declassified after 2-3 years (or as soon as practicable), barring extraordinary circumstances. This would allow public oversight by providing the standards and rationales employed in making warrant determinations. Also, unlike FISC, the judges sitting on this body should not be elected for a part-time or short-term assignment. They should, like other judges in specialized courts, become subject matter experts in foreign intelligence surveillance warrants. This specialization should foster the speed and knowledge to ensure that government warrants can be decided with the requisite swiftness while carefully adhering to constitutional and legal safeguards.

The executive branch should closely abide by the rules set by the legislature and the judicial system's determinations. The executive branch should never bypass warrant requirements, as both the U.S. and UK have historically done. Nor should the judiciary be left out of the surveillance framework, which France has historically done. The executive branch should also be as transparent as possible. While they may not be able to provide details about individual investigations, they should continue to publish data related to the number of warrants authorized and the effectiveness of the programs. These transparency reports should provide adequate information to inform the public on the breadth

of government surveillance activities. There should also be an ombudsman that receives complaints at any point in the foreign intelligence process. If people are unjustly targeted and harmed, they should be able to seek redress through administrative or judicial bodies.

This process would prevent the most intrusive government programs from being implemented. For instance, the NSA and GCHQ hacking into corporate or telecommunication infrastructure and setting up "black boxes" to monitor mass data would violate these procedural requirements. They would inevitably be surveilling a multitude of individuals without a warrant, and it would not adhere to the legislature's individualized suspicion guidelines. Further, this should also remove the coercive elements we have seen from agencies like the NSA (recall the NSA threatening Yahoo with a $250,000 a day fine for not letting them bug their infrastructure). It would also, in theory, repeal other pieces of legislation or executive orders that have historically permitted mass surveillance. This would include much of the UK's surveillance legislation in recent years. Most importantly, there must be a legislative or judicial mechanism to ensure that the executive branch is adhering to these guidelines. This could take the form of independent committees between those two branches, or another independent watch group, which is mandated to ensure executive branch compliance with surveillance laws. While it would be ideal to trust the executive branch to abide by the law, history has shown that it is insufficient.

In fact, in each of the three countries examined, executive branch discretion historically facilitated the development of mass surveillance infrastructure. The United States saw this with various surveillance efforts conducted by law enforcement agencies post-WWII, such as COINTELPRO and Operation Chaos. More recently, it came in the form of the NSA unilaterally expanding the permissible bounds of the Patriot Act's surveillance, as was noted by the bills' author. There was similarly an absence of legislative mandates for the French DGSE's data collections and transfers under the Lustre agreement, as well as the British GCHQ's mass surveillance. The primary goal of these

executive branch agencies is to gather intelligence and protect national security, which–particularly in the case of mass surveillance–may not always align with protecting the civil liberties of domestic citizens. There needs to be checks and balances against these agencies' discretion, but more importantly, there must be mechanisms to ensure that these intelligence agencies are closely following those requirements.

B. Ensure Privacy Rights

The United States, UK, and France should better protect their citizens' privacy against the government. A suitable place to look for guidance would be the EU. The EU has historically appeared to be a staunch supporter of privacy rights. Article 8 of the ECHR explicitly recognizes privacy as a fundamental right. The Council of Europe Convention 108 goes a step further in ensuring data privacy. There is also relatively robust EU caselaw on mass surveillance.[376] The GDPR is potentially the landmark data privacy legislation globally. The countries discussed in this paper, however, have yet to follow this track.

In fact, in France and the UK things seem to be getting worse, with the UK currently being an archetypical surveillance state and perhaps the most invasive in Europe. Ironically, things seem to be getting better in the U.S., even though the U.S. remains one of the only nations without comprehensive data protections laws nor a constitutional guarantee of privacy. The U.S. should take steps to permanently codify privacy rights in the constitution and therefore provide a constitutional basis for data privacy legislation. For France and the UK, after centuries of surveillance and privacy rights violations, these governments should move towards ensuring that the fundamental liberty of privacy is guaranteed to their citizens. France and the UK are currently moving in the wrong direction, and it is a perfect time to change course.

Another key point is that while many countries constitutionally guarantee the right to privacy, the three countries examined do not. As

[376] *See* source cited *supra* note 351.

previously mentioned, the U.S. analog to constitutional privacy rights is the Fourth Amendment, but the Fourth Amendment does not mention "privacy." Nor does the 1958 French Constitution explicitly provide for privacy rights.[377] However, Article 9 of the French Civil Code does stipulate that "[e]veryone has the right to respect for his private life."[378] France is also bound by Article 8 of the ECHR and EU data protection laws like the GDPR. The UK does not have a codified constitution, but the Human Rights Act of 1998 incorporated Article 8 of the ECHR into UK law.[379] Out of the three countries, France appears to have the most privacy protections due to the ECHR, binding EU precedent, and Article 9 of the French Civil Code. It is possible that these protections contributed to France conducting less mass surveillance throughout the 20th and early 21st century.

It is difficult to determine whether the existence–or absence–of constitutional privacy rights has directly influenced the development of mass surveillance regimes in these three countries. The U.S. has the weakest privacy guarantees, yet FISA theoretically provided the most expansive protections–though rarely implemented in practice. Similarly, the U.S. has had the strongest rollback of mass surveillance in recent years, even without this constitutional protection. Nonetheless, this should not diminish the importance of protecting privacy rights at the highest level, whether that be constitutionally (in the United States and France) or through binding federal legislation (in the UK). This would provide an additional avenue for litigants to challenge mass surveillance regimes or vindicate being unjustly targeted by intelligence agencies.

A constitutional right to privacy may have led to *Clapper v. Amnesty International* being decided differently. Alternatively, the U.S. Supreme Court may have been more willing to accept cases based in

---

[377] *See* Priv. Int'l, U.N. Hum. Rts., Off. of the High Comm'r, The Right to Privacy in the French Republic 5 (29th sess. 2017) ("There is no specific personal data protection or privacy guarantee in the 1958 Constitution.").

[378] Code civil [C. Civ.] [Civil Code] art. 9 (Fr.) ("Everyone has the right to respect for his private life.").

[379] *See generally* Human Rights Act 1998, c. 42 (UK).

mass surveillance if there was a clear constitutional violation occurring. It could also provide a constitutional basis for GDPR-like legislation in the U.S., which could restrict data collection efforts by data processors. This would reduce the available avenues that U.S. intelligence agencies have to gather data on citizens. The presence of this privacy right could also equip litigants in France and the UK with additional weapons to successfully challenge the recent bills expanding mass surveillance. Although success on the merits in litigation is never guaranteed, expanding privacy protections could help balance the scales in favor of those conducting legal challenges to mass surveillance legislation.

Even with a guaranteed right to privacy in these jurisdictions, governments will likely seek exceptions based in national security for foreign intelligence surveillance. As previously mentioned, intelligence can be pertinent to national security but must be accompanied by the appropriate safeguards. Like other fundamental guarantees, there are limited situations where it can be abridged, but only if accompanied by reasonable individualized suspicion, a warrant, and the possibility for redress if errors occur. Ensuring a fundamental right to privacy is a necessary, but not sufficient, step that governments should take to prevent citizens from being arbitrarily subject to surveillance. Because of this, the recommendation for guaranteed privacy rights must be implemented in tandem with the oversight of foreign intelligence proposed in the previous section if indiscriminate mass surveillance is going to be defeated.

C. Protect Civil Liberties in the Face of Fear

In times of war or social unrest, citizens must demand that their governments do not carte blanche violate their civil liberties. Many things can be justified in war–stripping away the natural rights and fundamental liberties of people should not be one of them. Often, in each country, we saw the domestic surveillance of war dissidents and suppression of the media during times of war or unrest. These were inevitably used to target individuals based on affiliations deemed undesirable by the government, such as jews, socialists, laborers, suffragettes,

civil rights activists, and even Catholics. The prospect of war, or terrorism, does not permit the government to intrude on the privacy and free speech rights of its citizens. These intrusions suppress public opinion, silence public discourse, and can cause large segments of the population to suffer. It is on the masses to ensure that they stand up to government oppression, even when they may be afraid.

These emergency powers have also historically outlived the conflicts they were meant to address. In 2013, Edward Snowden was charged with violating the Espionage Act of 1917. This statute was enacted during WWI to protect the war effort, yet was weaponized against a mass surveillance whistleblower almost a century later. The Patriot Act similarly went well beyond its sundown provision after 9/11. The French Olympics Law authorizing AI mass surveillance is still in effect, even though the 2024 Olympics ended seven months ago. Often, in each of the three countries examined, the intelligence agencies were developed or expanded in the face of conflict or terrorism. Instead of these agencies being disbanded or diminished after this unrest ended, often they were reorientated towards domestic citizens with dissenting views on government activities.

Admittedly, there may be times of grave uncertainty that require an expansion of government surveillance efforts. But WWII ended eighty years ago. WWI ended over a century ago. The most recent full-scale civil war in these countries was in the U.S. and ended in 1865. If somehow these countries end up in another period of grave uncertainty, an expansion may be justified, but it should be rolled back as soon as the conflict is over. Each of these three countries are democracies and elected officials are subject to the will of their voters. People should stand up for their privacy rights and other civil liberties and ensure that the government does not overreach.

D. AI and Intelligence Surveillance

The use of AI should be embraced, but *extremely* cautiously. The French Olympics Law is a stereotypical example of AI being used in a

negative manner. There are several steps that can be taken to ensure the ethical use of AI in surveillance activities. Ethical guidelines should be published regarding the collections and analyzation of biometric data through AI. Mass surveillance generally should be abolished, not exasperated by the use of AI. AI-driven surveillance efforts seek to monitor massive segments of the population and make predictions about what people *might do*. From this arises the prospect of arbitrary enforcement and heightened scrutiny on minority groups. It also goes a step further than metadata retention, instead collecting and analyzing the real-time biometric (and personally identifiable) data of millions. AI-driven surveillance undermines the presumption of innocence by deciding guilt before any crime is committed. Few things are more Orwellian than machines constantly tracking you, predicting your next move, and waiting to catch you doing something wrong.

Of course, AI could be strategically employed in a positive manner if the appropriate safeguards are in place. AI facial recognition could be used to help locate a missing person through targeted facial recognition efforts supported by a warrant. It can help identify online human trafficking or financial crimes with speed that humans simply do not possess. It can process terabytes of legally acquired evidence in a criminal case to help identify patterns. AI can also monitor potential cybercrimes and reinforce data security infrastructure. But AI must be used with the appropriate safeguards of individualized suspicion, targeted efforts, and a warrant. Otherwise, the world will see the surveillance state–which each of these three countries are guilty of establishing–reaching powers and breadth never previously thought achievable.

Conclusion

Privacy, and by extension data privacy, should be viewed as a natural and fundamental civil liberty. Human and natural history has shown that this is a fundamental need for humans. In the U.S., UK, and France

we have seen the pendulum of mass surveillance swing back and forth, often being established in times of uncertainty but continuing well into the future. Mass surveillance undermines privacy rights, increases self--censorship, leads to intimidation-induced chilling effects on speech, undermines the freedom of assembly, and reduces trust in the state. All of this is done in the name of national security, but evidence indicates that mass surveillance does not make us safer and actively diverts resources from programs that could have.

There should be meaningful three-branch oversight of foreign intelligence surveillance supported by an ombudsman to receive complaints at any point in the process. Court decisions issuing warrant should be made public as soon as it is feasible to do so. Governments should guarantee the right to privacy, citizens should stand up for their rights even when they are afraid, and the use of AI should be done narrowly and with the appropriate safeguards. Society can achieve adequate foreign intelligence surveillance without abridging civil liberties, but it appears that some countries are headed in the wrong direction: now is the time to change course.