THE CHILLING OF RELIGIOUS LIBERTY IN THE AGE OF DIGITAL SURVEILLANCE

*Gineen K. Abuali**

I. INTRODUCTION

It is 5:50 in the morning in New York. Phones across the city buzz, playing the *Athan* and waking congregants up for *Fajr* prayer. For years, congregants relied on a phone app to notify them when it was time for their five daily prayers, unaware that at some point the app secretly sold their location data, making it easier for the government to track them. This app, Muslim Pro, which provides Muslims with tools like prayer times, geographic location in regard to Mecca, and a stream of religious content, allegedly sold the location of its Muslim users—data that eventually ended up in the hands of the US military.[1]

Across the river in New Jersey in a Federal Bureau of Investigation (FBI) facility, sits Pegasus, an Israeli spyware product that can crack the encrypted communications of smartphones.[2] The government purchased this product—described as a tool democracies use to spy on their citizens—for allegedly routine testing of new technologies.[3] Like the app, Pegasus is utilized to collect sensitive information about individuals.[4] For its part, the FBI secretly tried out Pegasus spyware without public knowledge, until a groundbreaking news investigation uncovered the scheme.[5]

The impact of this digital technology and spyware on religious communities in America, particularly Muslim communities, is an

* J.D. Candidate, 2024, Seton Hall University School of Law; B.A., Saint Peter's University.

[1] Joseph Cox, *How the U.S. Military Buys Location Data from Ordinary Apps*, VICE (Nov. 16, 2020, 10:35 AM), https://www.vice.com/en/article/jgqm5x/us-military-location-data-xmode-locate-x.

[2] Ronen Bergman & Mark Mazzetti, *The Battle for the World's Most Powerful Cyberweapon*, N.Y. TIMES (June 15, 2023), https://www.nytimes.com/2022/01/28/magazine/nso-group-israel-spyware.html.

[3] *Id.*

[4] *Id.*

[5] *Id.*

under-acknowledged but serious problem because the full ramifications of its broad scope are still unknown. But this technology has the power to collect sensitive information unlike anything seen before. This Comment argues that such digital surveillance programs jeopardize constitutional order and its pluralistic democracy, and simultaneously threaten to chill the free exercise of religion.

Most scholarship discusses government infiltration of Muslim communities as a form of spying and policing, and some scholarship explores the use of modern technology to do the same. Many legal writers have focused on how this surveillance implicates freedom of speech and the Fourth Amendment.[6] Few, however, have analyzed how the digital surveillance of these communities chills religious practice, and it is important not to lose sight of the religious freedom implications of such government conduct because religious freedom not only protects religious practice but also reinforces other core civil liberties. This Comment fills that gap and examines the religious freedom implications of the government's exploitation of technologies like Pegasus and Muslim lifestyle apps like Muslim Pro—a significant concern as communication becomes increasingly globalized and groups continue to rely on digital tools to facilitate religious practice.

This Comment analyzes how new technology facilitates spying on religious minorities, as well as the ways in which the convergence of technology and government surveillance allows for the new but same old policing of these communities. It sets out broader questions about how Americans should grapple with these modern forms of surveillance and their particular ramifications for democracies. Ultimately, it argues that this overlooked aspect of policing and surveillance in the digital age chills religious practice. Specifically, digital technology and new forms of government surveillance have emerged as far-reaching barriers that prevent Muslims from fully practicing their religion as the First Amendment affords them.

Part II of this Comment recounts prior periods where local law enforcement and federal national security entities committed targeted surveillance of particular groups in the United States, like Black individuals and Muslims. Part III describes digital surveillance and its various forms. Part IV explores digital surveillance's implications for religious liberty and legal barriers litigants will face in challenging such

---

[6] *See, e.g.*, *infra* notes 69, 80 and accompanying text; Ana Pajar Blinder, Comment, *Don't (Tower) Dump on Freedom of Association: Protest Surveillance Under the First and Fourth Amendments*, 111 J. CRIM. L. & CRIMINOLOGY 961, 968 (2021).

practices, including demonstrating standing and a chilling of their rights under the Free Exercise Clause. Part V provides solutions and assesses where to go from here, with a particular focus on addressing surveillance in places that call themselves democracies. Part VI briefly concludes.

II. HISTORY OF GOVERNMENT SURVEILLANCE OF UNDERREPRESENTED COMMUNITIES

Understanding the history of government surveillance of Americans in the name of national security in the United States is important for a number of reasons. It helps explain the roots of such surveillance and the government's often repetitive justifications. Even more, it demonstrates how the cycle never ends. The victims may not all look the same, but the name of the game is the same. The following sections trace government surveillance of Martin Luther King, Jr., in Section A, and surveillance of Muslims following September 11, 2001, in Section B, as two examples where the government deployed its surveillance apparatus against unpopular or minority groups wrongly perceived as threats. The surveillance of King is particularly poignant because it demonstrates the religious undercurrents of his targeting beyond his status as a civil rights leader, but as a religious leader targeted in his place of worship.

A. *Broader History of Surveillance of Particular Groups and Activists in America*

One of the most disregarded and untold stories of American history is how the FBI surveilled King and other civil rights activists for years. During World War II, the FBI increased its efforts to investigate national security threats, which it apparently viewed as including King.[7] Under this broad definition, the FBI investigated civil rights leaders, as well as members of the Black Panthers and other groups viewed as threats.[8]

The FBI targeted King beginning in December 1955 following his participation in the Montgomery Bus Boycott.[9] From then on, the

---

[7] *Federal Bureau of Investigation (FBI)*, THE MARTIN LUTHER KING, JR. RSCH. & EDUC. INST. [hereinafter *FBI*], https://kinginstitute.stanford.edu/encyclopedia/federal-bureau-investigation-fbi (last visited Sept. 27, 2023).

[8] *Id.*; Virgie Hoban, *"Discredit, Disrupt, and Destroy": FBI Records Acquired by the Library Reveal Violent Surveillance of Black Leaders, Civil Rights Organizations*, BERKELEY LIBR. (Jan. 18, 2021), https://www.lib.berkeley.edu/about/news/fbi.

[9] *Id.*

government surveilled King and employed other covert tactics until his death.[10] Beginning in 1956, the FBI formed its Counterintelligence Program (COINTELPRO), in the words of FBI Director J. Edgar Hoover, "to spy on and 'neutralize' all 'radical or immoral activity.'"[11] The government used the program against politically unpopular groups that it feared, which included the Black Panthers.[12] As part of the program, the agency infiltrated organizations, spread false information, incited violent actions and chaos at gatherings, and even carried out assassinations.[13]

The FBI targeted King in particular because it suspected he was a Communist.[14] It even surveilled King's religious activities. Not only did the FBI bug his church and record his speech, but local law enforcement also kept the tapes secret "for three decades before releasing them."[15] The federal agency used about fifteen hidden microphones at one point, along with other concealed devices, and also infiltrated the Southern Christian Leadership Conference with informants.[16] King's surveillance was the rule, not the exception. During the 1960s and 1970s, police files overflowed "with the names of anti-Vietnam War protestors, Black nationalists, the so-called New Left, women's liberation groups, and others" whom the FBI considered suspicious.[17] Other government bodies beyond law enforcement were involved. For example, the Internal Revenue Service flagged dissidents' tax returns, and military intelligence infiltrated groups looking for signs of subversion.[18] More than seventy-five lawsuits arose

---

[10] *Id.*

[11] Nancy Murray & Sarah Wunsch, *Civil Liberties in Times of Crisis: Lessons from History*, 87 MASS. L. REV. 72, 81 (2002).

[12] Hoban, *supra* note 8.

[13] *Id.* Chicago police officers, with the FBI's assistance, assassinated Fred Hampton, chairman of the Black Panthers, while asleep in his bed, right after they assassinated Mark Clark, deputy defense minister of the Black Panthers, as he opened the door. JAKOBI WILLIAMS, FROM THE BULLET TO THE BALLOT: THE ILLINOIS CHAPTER OF THE BLACK PANTHER PARTY AND RACIAL COALITION POLITICS IN CHICAGO 180 (2013).

[14] *FBI*, *supra* note 7.

[15] Tom Lininger, *Sects, Lies, and Videotape: The Surveillance and Infiltration of Religious Groups*, 89 IOWA L. REV. 1201, 1211 (2004).

[16] *Id.*

[17] Murray & Wunsch, *supra* note 11, at 81.

[18] *Id.*

between 1964 and 1974 in response to police surveillance of political and social groups.[19]

This time period demonstrates the harm law enforcement monitoring of religious groups can cause, particularly "when law enforcement . . . lack[s] clear limits."[20] For example, in addition to surveilling King, the FBI made multiple efforts to block King's meetings with other religious leaders and groups, attempted to obstruct his publications, and tried to derail his efforts to raise donations for the Southern Christian Leadership Conference.[21] While at the time the chilling effect may have been muted or gone unrecognized because of secrecy, years later investigations recognized this surveillance for what it was—an effort to chill First Amendment activity.[22] Although this is not identical to claims of purely religious practice chilling, it is particularly noteworthy because religious practice, political organizing, and speech are all interconnected, protected activities that suffer when the government engages in surveillance. In 1976, the Senate Church Committee released its findings from a study of government intelligence operations, which documented how expression of views, associations with groups the government considered unpopular, and participation in peaceful protest, triggered government surveillance and retaliation.[23] Most surprisingly, the study confirmed that spying tended to chill First Amendment rights, such as free speech and association, and implied that this was the goal of the surveillance as "[i]ntelligence agencies . . . expressly attempted to interfere with those rights."[24] Because of this documented past, today vulnerable communities have more information and good reason to fear the government's surveillance. This documented past puts people on notice that fears of surveillance are not just wild conspiracy theories but reasonable because surveillance is a very real possibility. Additionally, it raises the question: if it happened in the 1960s, and as the next section shows, again after

---

[19] Lininger, *supra* note 15, at 1213 n.43 (citing John H.F. Shattuck, *Titling at the Surveillance Apparatus*, 1 C.L. REV. 59, 60 (1974)).

[20] *Id.* at 1213.

[21] MARVIN JOHNSON, AM. C.L. UNION, THE DANGERS OF DOMESTIC SPYING BY FEDERAL LAW ENFORCEMENT: A CASE STUDY ON FBI SURVEILLANCE OF DR. MARTIN LUTHER KING 6–7 (2002), https://www.aclu.org/sites/default/files/FilesPDFs/mlkreport.pdf.

[22] S. REP. NO. 94-755, at 290–91, 395 (1976).

[23] *Id.* at 291.

[24] *Id.* at 17, 290–91.

September 11, 2001, what are the implications for the twenty-first century as technology grows in sophistication?

B. *Focus on the NYPD and Mosque Surveillance*

Large-scale surveillance of Muslims following September 11, 2001, was a hallmark of local law enforcement's development of counterterrorism programs in cities across the country. As Muslims automatically became suspects of terrorism, mosque surveillance and infiltration in many areas with large Muslim populations became the norm. The New York Police Department (NYPD) became notorious for its counterterrorism program, surveilling not only individuals and local Muslim community leaders, but also mosques, businesses, and Muslim student associations on college campuses.[25] Surveillance extended beyond the borders of New York to its neighboring states of New Jersey, Pennsylvania, and Connecticut.[26] Law enforcement justified this widespread surveillance as a necessary preventative measure to stop future terrorism.[27] While the NYPD utilized video and photo surveillance to spy on Muslim groups, it became infamous for its use of "'mosque crawlers' to observe activities within mosques as well as 'rakers,' plain clothed officers responsible for listening to conversations at Muslim restaurants and businesses."[28]

The NYPD collected vast personal information on Muslims never accused of any crimes, including license plate numbers of those who parked at mosques, photographs, and even information obtained from monitoring colleges.[29] Performing regular daily tasks could trigger surveillance if one was Muslim, or suspected of being Muslim.[30] "The only thing these individuals had in common was that they all belonged to the Islamic religion."[31]

---

[25] *See* Aimee Blenner, Comment, *Watch Out: You're Being Watched (If You're Muslim)*, 16 RUTGERS J.L. & RELIGION 618, 618 (2015).

[26] *Id.*

[27] *Id.*

[28] *Id.*

[29] *Factsheet: The NYPD Muslim Surveillance Program*, ACLU (June 17, 2013), https://www.aclu.org/other/factsheet-nypd-muslim-surveillance-program; David Crary, *AP Series About NYPD Surveillance Wins Pulitzer*, ASSOCIATED PRESS (Apr. 16, 2012), https://www.ap.org/ap-in-the-news/2012/ap-series-about-nypd-surveillance-wins-pulitzer#:~:text=In%2520a%2520series%2520of%2520articles,law%25.

[30] *See* Matt Apuzzo & Joseph Goldstein, *New York Drops Unit That Spied on Muslims*, N.Y. TIMES (Apr. 15, 2014), http://www.nytimes. com/2014/04/16/nyregion/police-unit-that-spied-on-muslims-is-disbanded.html.

[31] Blenner, *supra* note 25, at 619.

Surveillance in New Jersey offers a particularly potent example. There, "police monitored [a minimum of] twenty mosques, fourteen restaurants, eleven retail stores, two grade schools, and two student groups."[32] Newark, a city with a significant Black Muslim population, received particular attention.[33] This exposes how communities doubly marginalized on the basis of both race and religion battle increased risks of surveillance.

Surveillance extended beyond the local level. In 2003, FBI leadership "ordered all fifty-six of the FBI's branch offices to count the . . . mosques within their . . . boundaries."[34] The government first claimed this was a strategic, "proactive investigation[] of potential terrorists."[35] After groups objected due to concerns about burdening religious freedom, the FBI changed its tune, publicly stating that defending Muslims against hate crimes required an inventory of mosques.[36] Since then, the agency has moved significantly beyond mosque-counting and has focused efforts on infiltrating mosques in the United States and other countries.[37] To do this, the FBI deployed "confidential informants, undercover agents, surveillance cameras, flyovers, and subpoenas for phone records," as just a few of its investigative techniques.[38]

Legal scholars, advocates, and community members argue that mosque surveillance and infiltration since 2001 has impacted Muslims' religious freedom as many have stopped attending religious services in fear of terrorism accusations.[39] Mosque infiltration has become so

---

[32] *Id.*

[33] Charles Toutant, *Third Circuit Considers NYPD Muslim Surveillance Suit*, N.J. L.J. (Jan. 14, 2015, 5:09 PM), https://www.law.com/njlawjournal/almID/1202715191998.

[34] Lininger, *supra* note 15, at 1204 (alteration in original).

[35] *Id.* at 1204–05.

[36] *Id.* at 1205.

[37] *Id.* at 1207; *see also* Leila Rafei, *How the FBI Spied on Orange County Muslims and Attempted to Get Away with It*, ACLU (Nov. 8, 2021), https://www.aclu.org/news/national-security/how-the-fbi-spied-on-orange-county-muslims-and-attempted-to-get-away-with-it; Eliott C. McLaughlin, *FBI Planting Spies in U.S. Mosques, Muslim Groups Say*, CNN (Mar. 20, 2009), https://www.cnn.com/2009/US/03/20/fbi.muslim.groups.

[38] Lininger, *supra* note 15, at 1205–07 (footnotes omitted); AM. C.L. UNION, BLOCKING FAITH, FREEZING CHARITY: CHILLING MUSLIM CHARITABLE GIVING IN THE "WAR ON TERRORISM FINANCING" 69 (2009) [hereinafter BLOCKING FAITH, FREEZING CHARITY] (describing how law enforcement approached Muslims to serve as mosque informants to monitor charitable giving).

[39] *See, e.g.*, Teresa Watanabe & Paloma Esquivel, *L.A. Area Muslims Say FBI Surveillance Has a Chilling Effect on Their Free Speech and Religious Practices*, L.A. TIMES

prevalent that some Muslims simply "assume they are under surveillance as they fulfill their religious obligations."[40] In fact, "[g]overnment informants have ensnared numerous, seemingly hapless and unsophisticated young men such that Muslims no longer know whom they can trust among each other."[41] Allegations of the government's use of informants to entrap mosque attendees in terrorism schemes and phony plots have fostered suspicion in local mosques.[42] Indeed, counterterrorism efforts attack social relationships by stunting "the vibrancy and development of civil society" in Muslim communities.[43] In a Pulitzer Prize-winning 2011 report, journalists for the Associated Press conducted an investigation into the NYPD's spying program and its impact on Muslim communities.[44] A reporter described what community members viewed as a typical occurrence:

> Strangers loitered across the street from the [Muslim-owned] cafe in this Brooklyn neighborhood. Quiet men would hang around for hours, listening to other [predominantly Muslim] customers. Once police raided the barber shop next door, searched through the shampoos and left. Customers started staying away for fear of ending up on a blacklist, and eventually Ahmad had to close the place.[45]

(Mar. 1, 2009, 12:00 AM), https://www.latimes.com/archives/la-xpm-2009-mar-01-me-muslim1-story.html; Saher Khan & Vignesh Ramachandran, *Post-9/11 Surveillance Has Left a Generation of Muslim Americans in a Shadow of Distrust and Fear*, PBS, https://www.pbs.org/newshour/nation/post-9-11-surveillance-has-left-a-generation-of-muslim-americans-in-a-shadow-of-distrust-and-fear (Sept. 16, 2021, 5:30 PM); Hassan v. City of New York, 804 F.3d 277, 287–89 (3d Cir. 2015).

[40] Sahar F. Aziz, *Caught in a Preventive Dragnet: Selective Counterterrorism in a Post-9/11 America*, 47 GONZ. L. REV. 429, 433 (2012).

[41] *Id.*

[42] *See* William Glaberson, *Newburgh Terrorism Case May Establish a Line for Entrapment*, N.Y. TIMES (June 15, 2010), https://www.nytimes.com/2010/06/16/nyregion/16terror.html (detailing allegations that a government informant entrapped Muslim youth with promises of money and luxuries in bombing schemes, despite the young men's ill-equipment to plan such schemes).

[43] Aziz, *supra* note 40, at 434.

[44] *See* Crary, *supra* note 29; Matt Apuzzo et al., *With CIA Help, NYPD Moves Covertly in Muslim Areas*,
ASSOCIATED PRESS (Aug. 24, 2011), https://www.nbcnewyork.com/news/local/with-cia-help-nypd-moves-covertly-in-muslim-areas/1926933.

[45] Chris Hawley, *Law May Not Be on Muslims' Side in NYPD Intel Case*, ASSOCIATED PRESS (Nov. 7, 2011, 11:31 PM), https://www.sandiegouniontribune.com/sdut-law-may-not-be-on-muslims-side-in-nypd-intel-case-2011nov07-story.html.

Scholars, including Professor Sahar Aziz, have argued that this rampant surveillance not only impacts social relationships but also attacks individual civil liberties by "chill[ing] religious freedom rights and deter[ring] Muslims from fully practicing their faith."[46] Specifically, Muslim community leaders report that fear of inviting government surveillance led to "a reduction in attendance at mosques, a change in the language used at worship services, a [reduction] in [donations] to Muslim charities, and a [decimation] of trust and good will"—factors "essential to the vitality of a religious community."[47] Muslim individuals fear that visiting mosques or visibly expressing their Muslim identities may make them targets of an FBI investigation.[48]

The impact is not just theoretical. In 2009, the American Civil Liberties Union (ACLU) published a report detailing how worshippers were less willing to donate to their mosques and Muslim charities, despite a religious obligation to give charity, because of a pervasive fear that the government may implicate them in a terrorism investigation.[49] Donors were concerned "that they [could not] find a 'safe' Muslim charity to which they [could] donate without fear of reprisal."[50] These government intrusions have compromised the sense of privacy and security necessary for religious practice.[51]

Congressional advisory panels also echoed these concerns. The Gilmore Commission ("Commission"), formally the "Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction," was a congressional commission that ran from 1999 to 2004.[52] Chaired by former governor of Virginia, James Gilmore III, the Commission in 2003 focused on electronic surveillance and warned that, following September 11, increased electronic surveillance may chill freedom of religion.[53] The Commission emphasized that the legal system did not anticipate military intelligence gathering designed to aid law enforcement or

---

[46] Aziz, *supra* note 40, at 435.

[47] Lininger, *supra* note 15, at 1233–34 (alteration in original) (footnotes omitted).

[48] *Id.* at 1234.

[49] BLOCKING FAITH, FREEZING CHARITY, *supra* note 38, at 89.

[50] *Id.* at 92.

[51] Lininger, *supra* note 15, at 1236.

[52] *Gilmore Commission*, RAND, https://www.rand.org/nsrd/terrpanel.html (last visited Oct. 20, 2023).

[53] Lininger, *supra* note 15, at 1235.

military homeland defense missions.[54] As such, the Commission stressed it was "essential for the Congress to legislate and for the Department of Defense to implement through clear procedures the limitations on the use of . . . advanced technology monitoring inside the United States."[55] To enhance both security and liberty, the Commission recommended a bipartisan and independent oversight board to advise on any statutory or regulatory changes or implementation of anti-terrorism procedures that implicate civil liberties, even unintentionally.[56] According to the Homeland Security National Preparedness Task Force, the government adopted 146 recommendations, in whole or in part.[57]

III. WHAT IS DIGITAL SURVEILLANCE?

Masquerading as "sophisticated" technology, the use of digital surveillance and spyware to target Muslims collectively as national security threats based upon their religion is simply a new form of the same old tactics that discourage Muslims from fully realizing the freedom of religion the Constitution affords them. Like physical surveillance or infiltration, digital surveillance, such as tracking digital donations or religious speech, can impact the way individuals pursue religious activities.[58] Unlike physical surveillance, digital surveillance has the potential to be limitless because of the multiple forms it can take.[59]

Surveillance is "government efforts to gather information about people from a distance, usually covertly and without entry into private spaces."[60] Mosque infiltration, however, was just the opposite. There,

---

[54] ADVISORY PANEL TO ASSESS DOMESTIC RESPONSE CAPABILITIES FOR TERRORISM INVOLVING WEAPONS OF MASS DESTRUCTION, FORGING AMERICA'S NEW NORMALCY: SECURING OUR HOMELAND, PRESERVING OUR LIBERTY 23 (2003).

[55] *Id.*

[56] *Id.*

[57] HOMELAND SEC. NAT'L PREPAREDNESS TASK FORCE, CIVIL DEFENSE AND HOMELAND SECURITY: A SHORT HISTORY OF NATIONAL PREPAREDNESS EFFORTS 25 (2006), https://biotech.law.lsu.edu/blog/dhs-civil-defense-hs-short-history.pdf.

[58] *See* BLOCKING FAITH, FREEZING CHARITY, *supra* note 38, at 89.

[59] *See, e.g.*, Stephen Shankland, *Pegasus Spyware and Citizen Surveillance: Here's What You Should Know*, CNET (July 19, 2020, 8:49 AM), https://www.cnet.com/tech/mobile/pegasus-spyware-and-citizen-surveillance-what-you-need-to-know (describing how users can secretly install Pegasus and spy).

[60] CHRISTOPHER SLOBOGIN, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT 3 (2007), https://doi.org/10.7208/chicago/9780226762944.001.0001.

the NYPD entered arguably one of the most private spheres in an individual's life—their house of worship. Digital surveillance takes this covertness to another level. Perhaps digital surveillance is best defined not by a limited set of activities, but on a spectrum. Regardless, efforts have been made to at least define its contours.[61] Based on these combined definitions, digital surveillance (1) does not need to occur in person and can be remotely accessed; (2) entails the use of a product, service, or electronic technology to gain unauthorized access to a network, or to collect, intercept, identify, track, or record sensitive data and other identifying information; (3) can occur without consent; and (4) is extremely broad.[62] The following sections explore how the government deploys various forms of digital surveillance technology. Section A discusses the intersection of surveillance and social media, while Section B provides an overview of Muslim Pro and Pegasus.

A. *Social Media and Surveillance*

Plaintiffs challenging government surveillance of mosques focused their allegations on *physical* government surveillance.[63] This includes many of the tools and tactics that became familiar during the height of COINTELPRO in the 1960s and 1970s and that continued to be used against Muslim communities in the twenty-first century.[64] Such tools include informants, the deployment of "rakers" and "mosque crawlers" to infiltrate Muslim communities, searches of physical property, and wiretaps.[65] These were the surveillance tools of choice prior to social media's rise in 2006.[66] Since that development, reliance upon the old tools is less necessary, since the government can easily gather a host of information online.

The digital surveillance used on social media sites is known as data analytics, which includes predictive policing systems and other

---

[61] *See id.*; ISHAN SHARMA, FED'N OF AM. SCIENTISTS, A MORE RESPONSIBLE DIGITAL SURVEILLANCE FUTURE 5 (2021), https://uploads.fas.org/2021/02/Digital-Surveillance-Future.pdf; 50 U.S.C. § 1801(f); U.S. Dep't of Just., Crim. Res. Manual § 1077 (2020), https://www.justice.gov/archives/jm/criminal-resource-manual-1077-electronic-surveillance.

[62] *See* SLOBOGIN, *supra* note 60, at 3; SHARMA, *supra* note 61, at 5; Crim. Res. Manual § 1077.

[63] *Cf., e.g.*, *infra* notes 153, 176.

[64] *See Factsheet: The NYPD Muslim Surveillance Program*, *supra* note 29.

[65] *Factsheet: The NYPD Muslim Surveillance Program*, *supra* note 29; Sahar F. Aziz & Khaled A. Beydoun, *Fear of a Black and Brown Internet: Policing Online Activism*, 100 B.U. L. REV. 1151, 1173, 1178 n.160 (2020).

[66] Aziz & Beydoun, *supra* note 65, at 1173.

analytical tools that can derive information about identifiable individuals.[67] Today, law enforcement collects considerable intelligence about Muslims "through mining of social media data without the need for judicial warrants."[68] In the social media context, the government can more easily skirt constitutional restraints, like the requirement of a warrant, because information may be posted publicly. In this context, Fourth Amendment questions are different because social media is a platform where individuals post information for public consumption, so there is no "reasonable" expectation of privacy.[69] Depending on the circumstances, a private account can assure more protection, but not always, as police officers can use various tactics to disregard privacy settings, including "befriending" private social media users who accept an undercover officer's follow request.[70] Unsurprisingly, this is reminiscent of law enforcement's use of undercover informants in mosques who also attempted to "befriend" local Muslims for information gathering. Social media mining is thus one example of how digital surveillance expanded the dangerous potential for overreaching by allowing the government to reach more people with fewer Fourth Amendment restrictions.

As scholars have argued, practical limits on monitoring, like time and money, once restricted physical surveillance.[71] Notably, Rachel Levinson-Waldman of the Brennan Center for Justice stated surveillance technology continues to grow in sophistication and ease, broadening the amount of data that can be reached and increasing accessibility at the same time as it "lower[s] the bureaucratic barriers to privacy intrusions and creat[es] opportunities for near-frictionless surveillance that the Founders could not have envisioned."[72] There is

---

[67] SHARMA, *supra* note 61, at 5.

[68] Aziz & Beydoun, *supra* note 65, at 1173.

[69] The critical question is whether someone has a reasonable expectation of privacy when using social media. When social media users set their accounts to public, the Fourth Amendment will not protect the users' posts and a warrant will not be required because anyone can view them. *See* Yuval Simchi-Levi, *Search Warrants in the Digital Age*, 47 HOFSTRA L. REV. 995, 999–1000 (2019).

[70] Courts have sided with police in instances where government actors created fake accounts and befriended social media users who set their accounts to private or convinced friends of private users to share information with police. *See, e.g.*, M. Jackson Jones, *Shady Trick or Legitimate Tactic—Can Law Enforcement Officials Use Fictitious Social Media Accounts to Interact with Suspects?*, 40 AM. J. TRIAL ADVOC. 69, 71 (2016).

[71] Rachel Levinson-Waldman, *Government Access to and Manipulation of Social Media: Legal and Policy Challenges*, 61 HOW. L.J. 523, 524 (2018).

[72] *Id.*

a "revolution" happening online where law enforcement uses digital technology to monitor the social media profiles of individuals and "build . . . networks of connected individuals."[73] Today, the surveillance programs at issue in the early 2000s have transitioned into online counter-radicalization programs that police online posts and interactions and exploit such content for investigations, information gathering, and intelligence.[74]

A survey of five hundred law enforcement agencies in 2016 revealed that 75 percent reported utilizing social media to solicit crime tips and nearly 75 percent reported using it to track public sentiment and gather information for investigations.[75] While it may be argued that using information in the public domain for things like tips is perfectly all right, there is a fine line. A difference exists between using available information about suspected individuals for investigations and targeting specific individuals simply because of their identity, which is reminiscent of mosque surveillance.

What does the combination of this history and technological government ability mean for social media users most at risk because of their social identities or religious beliefs? Consciousness of government surveillance because of one's religion causes anxiety in the Muslim community "and adversely [impacts] how they outwardly worship and outwardly express their religious identity and self-identity."[76] This may not influence Muslims the same way as physical surveillance, such as causing them to stop visiting their houses of worship. But it does chill targeted communities by requiring them to change their worship to avoid surveillance. This raises important questions about what legal remedies people subjected to such practices may have to enforce their First Amendment rights. Those issues are explored below.

B. *The Muslim Pro Case and Pegasus*

Muslim Pro is a Muslim lifestyle app downloaded over 150 million times globally.[77] The government's interaction with Muslim Pro demonstrates how an app used to collect the location data of Muslim users ended up in the hands of the US government and military

---

[73] *Id.* at 523.

[74] Aziz & Beydoun, *supra* note 65, at 1173, 1178 n.160.

[75] Levinson-Waldman, *supra* note 71, at 524.

[76] Aziz & Beydoun, *supra* note 65, at 1176.

[77] *Muslim Pro: Digital Home for all Things Muslim*, MUSLIMPRO, https://www.muslimpro.com (last visited Oct. 20, 2023).

without a warrant ("Muslim Pro Case"). The app reminds users when to pray their five daily prayers, tells them what direction Mecca is in to properly position their prayers, allows them to read and listen to the Quran, and provides them with access to their daily supplications among a number of other features.[78] In 2020, Vice uncovered that for years the US military bought the location data of Muslim Pro users around the world for counterterrorism purposes.[79] The military did not buy the location data directly from Muslim Pro.[80] Instead, the scheme was much more covert: "Muslim Pro sent users' private location data to a data broker company called X-Mode, which sold the information to contractors, and thus by extension, the US military, which claims to use the information for counterterrorism purposes."[81]

Senator Ron Wyden's office already kept a keen eye on the data broker industry when the revelations became public.[82] It then expanded its investigation to Muslim Pro.[83] The Wyden investigation confirmed X-Mode's sale of data collected from phones in the United States to the military through defense contractors.[84] Wyden's office obtained this information in a September 2020 call with X-Mode.[85] The US Special Operations Command also confirmed that it uses location data like this to carry out its missions.[86] Although X-Mode anonymizes the data before sale, "the information [it collects] is so precise that individuals are easily identifiable."[87] Moreover, the collected data at issue comes from an app targeted at a particular religious community for a religious purpose. "Thus, even if technically anonymized, the data inevitably reveals information about religious associations since Muslim Pro users are largely Muslim."[88]

---

[78] Cox, *supra* note 1.

[79] *Id.*

[80] *See* Isabelle Canaan, *A Fourth Amendment Loophole?: An Exploration of Privacy and Protection Through the Muslim Pro Case*, 6 COLUM. HUM. RTS. L. REV. ONLINE 95, 98 (2022).

[81] *Id.* (alteration in original).

[82] Johana Bhuiyan, *Muslims Reel Over a Prayer App that Sold User Data: "A Betrayal from Within our Own Community"*, L.A. TIMES (Nov. 23, 2020, 11:57 AM), https://www.latimes.com/business/technology/story/2020-11-23/muslim-pro-data-location-sales-military-contractors.

[83] *See id.*

[84] *Id.*

[85] Cox, *supra* note 1.

[86] Canaan, *supra* note 80, at 95.

[87] *Id.* at 104.

[88] *Id.* at 105.

Pegasus is a digital surveillance tool in the form of spyware that can collect the information of smartphone owners without their consent.[89] Spyware is powerful technology with the ability to overcome encryption protecting data sent over the internet to directly reveal countless information about an individual's life, such as emails, texts, and photos.[90] Pegasus can be utilized without a target needing to ever open anything, like a document or link, because it can be installed remotely.[91] Notably, Pegasus uses "zero click" attacks to exploit vulnerabilities in software like iMessage or WhatsApp and silently install the software.[92] The spyware reveals everything to whoever is controlling it, including contact lists, texts, photographs, videos, and emails, and Pegasus also can create new recordings secretly by turning on a phone's recording devices.[93]

Israeli cyber-arms company NSO Group created Pegasus, and NSO Group sold the product to governments on a subscription basis for almost a decade with the promise that it can crack the encrypted communications of iPhone and Android smartphones, a feat that not even government intelligence agencies could achieve.[94] According to the company's website, "NSO Group licenses its products only to government intelligence and law enforcement agencies for the sole purpose of preventing and investigating terror and serious crime."[95] The company also says the purpose of its products is to help

---

89 *See* Shankland, *supra* note 59.

90 *Id.*

91 *Id.*

92 *Id.*; *see also* BILL MARCZAK ET AL., CITIZEN LAB, FORCED ENTRY: NSO GROUP IMESSAGE ZERO-CLICK EXPLOIT CAPTURED IN THE WILD 1, 3 (2021), https://tspace.library.utoronto.ca/bitstream/1807/123970/1/Report%23143—forcedentry.pdf (detailing how Pegasus exploited a vulnerability in iMessage to infect Apple devices). WhatsApp is just one company that recently sued NSO Group accusing it of unlawfully using the app to install spyware on users' devices. Lawrence Hurley, *Supreme Court Allows WhatsApp Lawsuit over 'Pegasus' Spyware to Move Forward*, NBC NEWS (Jan. 9, 2023, 9:34 AM), https://www.nbcnews.com/politics/supreme-court/supreme-court-allows-whatsapp-lawsuit-pegasus-spyware-move-forward-rcna64141. The NSO Group tried to use immunity reserved for state entities arguing it was immune from suit because it acted on behalf of foreign governments. *Id.* In January 2023, the Supreme Court rejected this argument, allowing the case to proceed. *Id.*

93 Shankland, *supra* note 59.

94 Bergman & Mazzetti, *supra* note 2.

95 *Governance*, NSO GROUP, https://www.nsogroup.com/governance (last visited Oct. 20, 2023).

governments as "terrorists and criminals have gone dark"[96] due to their use of advanced technology like encryption.

Despite the promises on NSO Group's website, researchers, in an effort to track the use of Pegasus, have found evidence of successful installations and other attempted installations of the spyware on the phones of journalists, activists, and others, indicating they were targets of secret surveillance.[97] Amnesty International's Security Lab carried out a forensic analysis of mobile devices belonging to human rights defenders and journalists and found "widespread, persistent and ongoing unlawful surveillance and human rights abuses perpetrated using NSO Group's Pegasus spyware."[98] Citizen Lab, a University of Toronto research lab focused on digital technology, confirmed government deployed this technology against religious leaders in Togo calling for reform.[99] Additionally, government deployed the technology against lawyers and activists in India belonging to minority and human rights groups in the country.[100] Reports also document Israel's suspected use of Pegasus against Palestinians in the West Bank.[101]

In January 2022, the *New York Times* published the findings of an investigation revealing that Pegasus may have been used even more broadly for dangerous ends.[102] According to the report, Saudi Arabia deployed it to spy on murdered journalist Jamal Khashoggi's communications and women's rights activists.[103] While NSO Group firmly denies their "technology was . . . associated in any way with the

---

[96] *Cyber Intelligence for Global Security and Stability*, NSO GROUP, https://www.nsogroup.com (last visited Oct. 20, 2023).

[97] Shankland, *supra* note 59.

[98] AMNESTY INT'L, FORENSIC METHODOLOGY REPORT: HOW TO CATCH NSO GROUP'S PEGASUS 6 (2021) [hereinafter FORENSIC METHODOLOGY REPORT], https://www.amnesty.org/en/documents/doc10/4487/2021/en/.

[99] *See* John Scott-Railton et al., *Nothing Sacred: Religious and Secular Voices for Reform in Togo Targeted with NSO Spyware*, THE CITIZEN LAB (Aug. 3, 2020), https://citizenlab.ca/2020/08/nothing-sacred-nso-sypware-in-togo.

[100] *See* Omer Benjakob, *The NSO File: A Complete (Updating) List of Individuals Targeted with Pegasus Spyware*, HAARETZ (Apr. 5, 2022), https://www.haaretz.com/israel-news/tech-news/2022-04-05/ty-article-magazine/nso-pegasus-spyware-file-complete-list-of-individuals-targeted/0000017f-ed7a-d3be-ad7f-ff7b5a600000.

[101] *Id.*

[102] *See* Bergman & Mazzetti, *supra* note 2.

[103] *Id.*

heinous murder of Jamal Khashoggi,"[104] there is also evidence that the US government, through the Central Intelligence Agency, paid for Djibouti to acquire Pegasus to help the American ally combat terrorism, raising concerns about human rights abuses in the country.[105]

Details of the United States' history with Pegasus domestically are also revealing, and allegedly, the spyware currently lies dormant in a New Jersey FBI facility.[106] The January 2022 *New York Times* story publicly revealed—for the first time—the details of the FBI's Pegasus purchase and testing.[107] The testing took place in June 2019 when Israeli engineers arrived at the New Jersey building and arranged their computer servers.[108] The test was a success:

> What they could see, minutes later, was every piece of data stored on the phone as it unspooled onto the large monitors of the Pegasus computers: every email, every photo, every text thread, every personal contact. They could also see the phone's location and even take control of its camera and microphone. [FBI] agents using Pegasus could, in theory, almost instantly transform phones around the world into powerful surveillance tools—everywhere except in the United States. . . . Israel, wary of angering Americans by abetting the efforts of other countries to spy on the United States, had required NSO to program Pegasus so it was incapable of targeting US numbers. This prevented its foreign clients from spying on Americans. But it also prevented Americans from spying on Americans.[109]

Even though Pegasus could not be used to spy on Americans, NSO Group also presented a new system to FBI officials in Washington.[110] The new system, called Phantom, could be used to hack any number located in America that the FBI sought to target.[111] This was because Israel provided a special license to NSO Group permitting Phantom to attack American numbers but only allowed American government

---

[104] *NSO News*, NSO GROUP, https://www.nsogroup.com/Newses/following-the-publication-of-the-recent-article-by-forbidden-stories-we-wanted-to-directly-address-the-false-accusations-and-misleading-allegations-presented-there.

[105] Bergman & Mazzetti, *supra* note 2.

[106] *Id.*

[107] *Id.*

[108] *Id.*

[109] *Id.* (alteration in original).

[110] *Id.*

[111] Bergman & Mazzetti, *supra* note 2.

agencies as clients.[112] Phantom would allow American agencies and law enforcement to gain access to phone data without the need for cooperation from phone service companies, such as Apple or Google.[113] Although the government and the company were in discussion for two years, "the FBI finally decided not to deploy the NSO weapons."[114] When the Biden Administration took over the White House, it placed NSO Group on the Department of Commerce's blacklist, explaining it had evidence the company provided spyware to governments that utilized it against dissidents, activists, and journalists beyond their borders to silence dissent.[115] This angered the Israeli government, which has ultimate say over NSO's sales, because America instituted the ban years after secretly testing Pegasus and other NSO products at home and allegedly giving them to "at least one [nation], Djibouti, with a record of human rights abuses."[116]

Pegasus poses particularly dangerous dormant threats to religious minorities because such groups are among those most likely to be government targets based upon past practices both in traditional surveillance using undercover informants and the surveillance documented in the Muslim Pro Case. Pegasus is a loaded weapon ready to replace the use of traditional surveillance directed at religious minorities. The Council of Europe echoed these concerns in a 2022 report, which highlighted the chilling effect Pegasus could have on freedom of religion and other related rights, like freedom of association.[117] Pegasus has the power to potentially intercept privileged communications with religious leaders, which could dissuade individuals from exercising their rights or joining groups with religious philosophies.[118] Part IV surveys key First Amendment principles and particular constitutional hurdles raised by digital surveillance under the First Amendment.

---

[112] *Id.*

[113] *Id.*

[114] *Id.* (alteration in original).

[115] Press Release, U.S. Dep't of Com., Commerce Adds NSO Group and Other Foreign Companies to Entity List for Malicious Cyber Activities (Nov. 3, 2021), https://www.commerce.gov/news/press-releases/2021/11/commerce-adds-nso-group-and-other-foreign-companies-entity-list.

[116] Bergman & Mazzetti, *supra* note 2.

[117] TAMAR KALDANI & ZEEV PROKOPETS, COUNCIL OF EUR., PEGASUS SPYWARE AND ITS IMPACTS ON HUMAN RIGHTS, 19 (2022), https://rm.coe.int/pegasus-spyware-report-en/1680a6f5d8.

[118] *Id.*

IV. DIGITAL SURVEILLANCE'S IMPLICATIONS FOR RELIGIOUS LIBERTY

A. *Protections the First Amendment Affords Religious Minorities*

The First Amendment to the US Constitution guarantees that "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances."[119] Freedom of religion is doubly protected in the First Amendment through two clauses—the Establishment Clause and the Free Exercise Clause.[120] While the Establishment Clause prohibits the government from establishing a state religion, the Free Exercise Clause restrains the government from enacting policies that would interfere with someone's religious practice.[121]

Government surveillance more closely impacts the Free Exercise Clause because history shows that surveillance implicates and changes how and where people practice their religion.[122] It also chills, or deters, religious exercise.[123] Although the language in the Free Exercise Clause sounds absolute, it is not.[124] In fact, courts once evaluated generally applicable laws or government action that hinder the free exercise of religion using the strict scrutiny test, but they no longer do.[125] Strict scrutiny is the highest standard used to examine government action, and it requires a challenged law or action to be in furtherance of a compelling government interest and use the least

---

[119] U.S. CONST. amend. I.

[120] *Id.*

[121] Nuzhat Chowdhury, Note, *I, Spy (But Only on You): Raza v. City of New York, The Civil Rights Disaster of Religious & Ethnic-Based Surveillance, and the National Security Excuse*, 46 COLUM. HUM. RTS. L. REV. 278, 300–01 (2015).

[122] Because this Comment focuses on the implications for religious practice, the Establishment Clause will not be discussed in depth.

[123] *See, e.g.*, Ed Stoddard, *U.S. Islamic Charities Feel Post 9/11 Heat*, REUTERS (July 20, 2007, 11:25 AM), https://www.reuters.com/article/us-usa-islam-charities/u-s-islamic-charities-feel-post-9-11-heat-idUSN1725413920070720; Neil MacFarquhar, *U.S. Muslims Reluctant to Donate to Charities—Americas—International Herald Tribune*, N.Y. TIMES (Oct. 30, 2006), https://www.nytimes.com/2006/10/30/world/americas/30iht-charity.3329887.html.

[124] *See* Chowdhury, *supra* note 121, at 294.

[125] *Compare* Sherbert v. Verner, 374 U.S. 398, 400–01, 403 (1963) (applying strict scrutiny to generally applicable laws), *with* Emp. Div. v. Smith, 494 U.S. 872, 874, 885–86 (1990) (holding that generally applicable laws no longer receive strict scrutiny).

restrictive means; in other words, it must be narrowly tailored.[126] The Supreme Court developed this test in the context of generally applicable laws inhibiting free exercise of religion in the 1963 case *Sherbert v. Verner*.[127]

In *Sherbert*, the issue concerned a generally applicable law that made individuals ineligible for state unemployment benefits if they did not accept suitable work.[128] Because the plaintiff objected to work on Saturdays, the plaintiff's Sabbath Day, the state denied the plaintiff the benefits.[129] The Court applied strict scrutiny to the generally applicable, neutral law.[130] The Court ruled in favor of the plaintiff, holding that the state had no compelling government interest to justify the imposition on the plaintiff's religious practice.[131]

Sherbert's reign was short-lived as in 1990, the Supreme Court limited the application of the *Sherbert* test in *Employment Division v. Smith*, holding that strict scrutiny no longer applies to generally applicable, neutral laws.[132] In *Smith*, the plaintiffs' employer fired the plaintiffs for consuming peyote at a religious ceremony of the Native American Church.[133] The state, which criminalized peyote use, denied the plaintiffs unemployment benefits since the state labeled peyote use as misconduct without exception for religious practice.[134] The Court held that a burden on one's free exercise could pass muster if it was an unintended result of generally applicable, neutral laws, and therefore, the government did not have to provide a compelling state interest as justification.[135] The Court reasoned that this situation is different from (1) circumstances where the state tries to regulate religion directly, which would get strict scrutiny;[136] or (2) hybrid situations where a state law or action implicates not only the Free Exercise Clause but also that clause in conjunction with another constitutional right, such as the freedoms of press, speech, and association.[137] In those two situations,

---

126 *Smith*, 494 U.S. at 894.

127 374 U.S. at 400–01.

128 *Id.*

129 *Id.* at 399, 401.

130 *See id.* at 406.

131 *Id.* at 404, 406–07.

132 494 U.S. 872, 874 (1990).

133 *Id.*

134 *Id.*

135 *Id.* at 879, 885.

136 *See id.* at 894, 897 (O'Connor, J., concurring).

137 *Id.* at 881–82.

the general applicability test would likely not apply.[138] Because a generally applicable criminal law resulted in the denial of unemployment benefits, the Court held that the state did not violate the plaintiffs' free exercise rights.[139]

As the Court in *Smith* explained, *Smith* would not apply to laws that directly target religious practice. Rather, strict scrutiny only applied to laws that directly targeted religion[140] or laws that arguably burden religious exercise directly.[141] In *Church of the Lukumi Babalu Aye v. City of Hialeah*, the Court applied strict scrutiny to a law that banned animal sacrifice for religious rituals because the Court found that the law, despite appearing neutral on its face, directly targeted religion since it intended to suppress Santeria worship.[142] The purpose was evident from what the Court described as a "religious gerrymander"—one of the only activities subject to the law was the religious exercise of Santeria members.[143] The law excluded almost all other slaughter of animals, including kosher slaughter and hunting.[144] Because of the singling out of religious practice for discriminatory treatment, the law could not be neutral.[145] Applying strict scrutiny, the Court struck down the law.[146]

Most recently, the Court appears to have reinvigorated the free exercise doctrine. In *Kennedy v. Bremerton School District*, the Supreme Court held that a school district violated a high school football coach's free exercise rights after it fired him for offering a personal prayer on the field following a game.[147] The Court applied strict scrutiny because it found the school district did not follow a neutral or generally applicable rule.[148] A government policy fails the neutrality test if it specifically targets religious practice, discriminates on its face, or if

---

138 *Smith*, 494 U.S. at 882.

139 *Id.* at 890.

140 *See* Church of the Lukumi Babalu Aye, Inc. v. City of Hialeah, 508 U.S. 520, 533 (1993).

141 *See* Kennedy v. Bremerton Sch. Dist., 142 S. Ct. 2407, 2415 (2022).

142 *Lukumi*, 508 U.S. at 534, 542.

143 *Id.* at 535 (quoting Walz v. Tax Comm'n of New York City, 397 U.S. 664, 696 (1970) (Harlan, J., concurring)).

144 *Id.* at 536.

145 *See id.* at 537–38.

146 *Id.* at 546.

147 142 S. Ct. 2407, 2415–16 (2022).

148 *Id.* at 2422.

discriminating against religious exercise is its object.[149] Additionally, a government policy will fail the general applicability requirement if it bans religious conduct while allowing secular conduct that similarly undermines the purported government interest, or if it allows for individualized exemptions.[150] The school district failed the neutrality test because the Court concluded that preventing religious practice was its object, and it failed the general applicability test because the school district did not apply postgame supervisory requirements in an evenhanded way to secular and non-secular activities.[151] The following part explores how the free exercise doctrine and cases challenging physical government surveillance can provide important considerations for future plaintiffs challenging digital government surveillance.

B. *Case Law Following NYPD Mosque Surveillance as a Guide to Challenging Digital Surveillance*

One of the most notorious cases challenging government surveillance provides important lessons for future plaintiffs. In response to rampant NYPD surveillance of mosques during the early 2000s described above,[152] Muslim community members brought suit challenging the surveillance and seeking relief for their alleged injuries in *Hassan v. City of New York*.[153] In 2012, civil rights organization Muslim Advocates filed suit on behalf of eleven plaintiffs, including a coalition of New Jersey mosques and the parent organization of the Muslim Student Associations (MSA) in New Jersey colleges.[154] The plaintiffs claimed they were targets of the NYPD's surveillance program following September 11, which also reached New Jersey.[155] The suit alleged that beginning in January 2002, the city of New York used the NYPD to secretly conduct the surveillance program to monitor Muslims' daily lives and their mosques, businesses, schools, and organizations.[156]

---

149 *Id.*

150 *Id.*

151 *Id.* at 2422–23.

152 *See* discussion *supra* notes 25–51.

153 Hassan v. City of New York, 804 F.3d 277, 284 (3d Cir. 2015).

154 *Id.* at 277.

155 *Id.* at 284.

156 *Id.* at 285.

According to the plaintiffs, the NYPD's actions chilled the exercise of religious rights because their fear of surveillance and false terrorism accusations led them to reduce their mosque attendance and other worship activities, including abstaining from openly discussing their faith with others or at MSA meetings and from praying in public places.[157] The organizational plaintiffs—mosques and charities—alleged that the surveillance program interfered with their duty to fulfill their missions, like protecting the confidentiality of their congregants, and harmed them financially.[158] Similarly, student organizations alleged they were unable to meet the spiritual needs of their members.[159]

The city moved to dismiss on the grounds that the plaintiffs lacked standing and failed to state a claim.[160] The district court granted the motion on both grounds.[161] As to standing, the district court held the plaintiffs failed to state a cognizable injury-in-fact or show causation.[162] The district court also held the plaintiffs failed to state a claim because it did not believe the surveillance stemmed from a desire to discriminate; rather, the court explained the more likely explanation was a purpose to track down budding terrorist conspiracies.[163]

On appeal, the Third Circuit reversed the district court's order granting the city's motion to dismiss, holding the plaintiffs both had standing to sue to vindicate their religious liberty and equal protection injuries and that they stated valid claims according to the First and Fourteenth Amendments.[164] The court rejected the city's arguments, even going so far as to say that some arguments bordered on frivolous.[165] As to standing, the court emphasized that unequal treatment and being singled out by the government is a cognizable

---

157 *Id.* at 287–88.

158 *Id.* at 288.

159 *Hassan*, 804 F.3d at 288.

160 *Id.*

161 *Id.*

162 *Id.* at 288–89.

163 *Id.* at 289.

164 *Id.* at 284–85.

165 *Hassan*, 804 F.3d at 308. The city argued that a New Jersey attorney general investigation exonerated the city from any violations of New Jersey law, and the court responded that it was "frivolous" that such an argument could triumph over a federal constitutional claim, reminding the city of *Marbury v. Madison* and that it is the judiciary's duty to lay down the law, not an executive from New Jersey. *Id.*

injury that has long been recognized.[166] The court also discarded the city's "halfhearted assertion" that successful First Amendment claims require overt hostility and prejudice.[167] While the city claimed it did not create its surveillance program to harm Muslim communities, the court explained that courts have repeatedly affirmed the principle that the Free Exercise and Establishment Clauses protect religious exercise from interference beyond animus.[168] In its powerful conclusion, the court quoted Justice Jackson's dissent in *Korematsu v. United States* and cautioned against targeting groups and the importance of abiding by the Constitution when confronting perceived threats to national security.[169] Before reversing the district court's decision, the court warned:

> What occurs here in one guise is not new. We have been down similar roads before. Jewish-Americans during the Red Scare, African-Americans during the Civil Rights Movement, and Japanese-Americans during World War II are examples that readily spring to mind. We are left to wonder why we cannot see with foresight what we see so clearly with hindsight.[170]

Although the Third Circuit did not rule on the merits of the plaintiffs' free exercise claims, following that decision, the city of New York settled the case in April 2018.[171] As part of the settlement, the NYPD agreed to halt its suspicionless surveillance based on religion or ethnicity, which the plaintiffs claimed was discriminatory and unlawful.[172] Additionally, the NYPD agreed to create a policy guide and to pay damages to plaintiffs who suffered income loss following their targeting by police and to plaintiffs who suffered from stigma and humiliation.[173]

---

166 *Id.* at 289.

167 *Id.* at 309.

168 *Id.* at 309.

169 *See id.*

170 *Id.*

171 *Hassan v. City of New York*, MUSLIM ADVOCS., https://muslimadvocates.org/court-case/hassan-v-city-of-new-york (last visited Sept. 28, 2023).

172 *Id.*

173 *Id.*

New York plaintiffs brought a similar challenge in *Raza v. City of New York*.[174] In 2013, the ACLU, New York Civil Liberties Union (NYCLU), and the CLEAR project at CUNY Law School filed suit on behalf of three religious community leaders, one charitable organization, and two mosques in federal court to challenge the NYPD's surveillance of Muslims.[175] The plaintiffs alleged that the NYPD violated and continued to violate their constitutional rights because of the NYPD's unlawful and unprovoked surveillance under what they called its "Muslim surveillance program."[176] The plaintiffs alleged violations of the Fourteenth Amendment's Due Process Clause, Free Exercise Clause, and Establishment Clause, and they brought a state constitutional freedom of exercise claim.[177] The District Court for the Eastern District of New York ruled that the plaintiffs were entitled to discovery concerning any NYPD programs or policies entailing investigation of Muslims as a group based on their religion because intent was central to the plaintiffs' equal protection claims.[178]

Ultimately, the case settled before the court ruled on the merits of the plaintiffs' claims. As part of the settlement, a federal judge ordered revisions to the Handschu Guidelines, the set of rules governing NYPD surveillance.[179] In addition to the appointment of a civilian representative to the NYPD to corroborate that all safeguards are followed, the revisions also included a religious discrimination policy, ending open-ended investigations through the imposition of time limits, and limiting the use of NYPD undercover and confidential informants.[180]

---

[174] *Raza v. City of New York - Legal Challenge to NYPD Muslim Surveillance Program*, ACLU, https://www.aclu.org/cases/raza-v-city-new-york-legal-challenge-nypd-muslim-surveillance-program (last visited Oct. 20, 2023).

[175] *Id.*

[176] Raza v. City of New York, 998 F. Supp. 2d 70, 73 (E.D.N.Y. 2013).

[177] *Id.*

[178] *Id.* at 81.

[179] *See Raza v. City of New York: Policing and Surveillance*, CLEAR, https://www.cunyclear.org/raza-v-city-of-new-york (last visited Oct. 20, 2023).

[180] *Id.*

C. *Application of the First Amendment to Digital Surveillance*

Hassan and *Raza* never ruled on the merits of the plaintiffs' free exercise claims. Thus, many issues remain unresolved when it comes to the First Amendment implications of government surveillance of Muslim communities, including what plaintiffs would need to show to succeed beyond defeating motions to dismiss free exercise claims and how deferential courts will be to the government when assessing the purpose of government programs or purported national security justifications. Those questions remain at issue with respect to digital surveillance. The courts' decisions in *Hassan* and *Raza* are nevertheless important and instructive because in rejecting the government's claim that the plaintiffs lacked standing, the courts recognized that First Amendment challenges to such practices may be cognizable in an area where injury is hard to show. This is particularly important to the digital surveillance context where injury may be even harder to show since covertness is more prominent in the sense that surveillance does not require the use of physical bodies. As digital surveillance continues to replace the in-person undercover surveillance at issue in *Hassan* and *Raza* more and more every day, the likelihood of chilling religious liberty is very real.[181] Digital surveillance efforts are an even greater threat and have unlimited potential to chill religious liberty perhaps because of the public ramifications of such efforts[182] or the ease of technological advancements.[183] Moreover, because digital surveillance programs are secretive, they more easily evade constitutional constraints.

Despite this, there are strategic paths plaintiffs can take to address these challenges. To successfully challenge digital surveillance as chilling religious liberty, victims must overcome three major hurdles: they need to (1) strategically frame a free exercise claim based on existing case law; (2) overcome standing barriers; and (3) demonstrate a chilling impact on their religious liberty.

---

[181] "The mining technology driving 'Big Data Policing' is *predictive* and being rapidly mainstreamed into the policing strategies of law enforcement departments in the United States, China, and countries beyond and in-between." Khaled A. Beydoun, *The New State of Surveillance: Societies of Subjugation*, 79 WASH. & LEE L. REV. 769, 776 (2022).

[182] *See, e.g.*, Hawley, *supra* note 45.

[183] "Through A.I., 'surveillance intermediaries' like Google and Facebook have remade our smartphones into 'one way mirrors' that mine our data for capital ends." Beydoun, *supra* note 181, at 775.

1. Strategically Framing a Free Exercise Claim

The free exercise doctrine can be organized into three categories: (1) generally applicable, neutral laws; (2) laws that directly target religious practice or laws that burden religious practice; and (3) as alluded to in *Smith*, hybrid actions that implicate another constitutional right.[184] Although it may be argued that digital surveillance is not a generally applicable, neutral law, the stronger argument for a constitutional challenge will likely be found in categories (2) or (3). This is because digital surveillance is so broad the government can argue it targets perceived threats who happen to be Muslim.[185] Although a counterargument can be made that the targets only became threats because of their religion, this may be difficult to show without documentation or records of some sort, especially in the national security context.

On the other hand, challengers could potentially try to argue that such government action is not a generally applicable, neutral law because government surveillance directly targets religious exercise.[186] The ruling in *Hassan* suggests that when the government perceives entire groups as national security threats because of their religion, courts may be more favorable to the argument that the government directly targeted those groups for their religion. At the same time, the Muslim Pro Case demonstrates direct targeting of religion because the government purchased the user data of an app made specifically for—and actually used by—Muslim users. In other words, it is a fair inference that by targeting Muslim lifestyle apps, the government directly targeted religion. Perhaps challengers can even make a *Lukumi*-like argument and argue that going after data from apps marketed to Muslims is a digital, modern-day religious gerrymander.[187] Challengers can go further and argue that because such Muslim lifestyle apps are meant to aid religious practice, like reading the Quran or providing prayer times, government surveillance chills such religious practice when users delete such apps due to surveillance.

The strongest constitutional challenge to government action compromising free exercise will likely need to be a hybrid action

---

184 *See* discussion *supra* Part IV.A.

185 *See, e.g.*, Lininger, *supra* note 15, at 1204–05 (describing how the FBI alleged counting mosques was necessary for proactive terrorism investigations).

186 *See* Emp. Div. v. Smith, 494 U.S. 872, 881–82 (1990).

187 *See* Church of the Lukumi Babalu Aye, Inc. v. City of Hialeah, 508 U.S. 520, 535, 542 (1993) ("[T]he texts of the ordinances were gerrymandered with care to proscribe religious killings of animals but to exclude almost all secular killings . . . .").

implicating another constitutional right because the Court left this route open as a possibility in its restrictive *Smith* ruling, and it provides the opportunity to show that a challenged action is severe, such that it attacks multiple rights at the same time.[188] Challengers of course must first show that such digital government surveillance is taking place, a difficult feat in and of itself. They will also need to show that they changed how they act and what they say after becoming aware of that surveillance. Before demonstrating this chilling impact, challengers will likely face standing barriers, such as difficulty showing injury.

2. Overcoming Standing Barriers

Victims must overcome standing issues in the first instance, which is a difficult feat with new technology. Although it will be difficult, *Hassan* and *Raza* demonstrate it is not impossible to show standing when one is challenging covert tactics. Standing requires plaintiffs to demonstrate three elements: injury-in-fact, causation, and redressability.[189] Injury to constitutional rights may afford standing, but the Court has been reluctant to recognize such an injury in the context of surveillance.[190] For example, in *Clapper v. Amnesty International USA* the Court rejected claims by human rights organizations and lawyers who feared the government would intercept their telephone and e-mail communications, concluding that hypothetical fears of surveillance, without evidence of a threat of certainly impending surveillance, is insufficient for standing.[191] The Court reaffirmed the reasoning of *Laird v. Tatum*, a case where plaintiffs claimed the Army's data gathering program could cause harm to them in the future,[192] holding that any subjective chilling of activities was too speculative and highly attenuated, and therefore, not adequate to show injury or causation.[193] Rather, the Court reasoned that injury requires a specific claim of objective, present harm or threat of specific, future harm.[194] Additionally, victims must trace their claimed injury to the government's actions, showing causation, and

---

188 *Smith*, 494 U.S. at 881–82.

189 *See generally* Clapper v. Amnesty Int'l USA, 568 U.S. 398 (2013) (explaining the issue of standing in the context of surveillance).

190 *See id.* at 414; Laird v. Tatum, 408 U.S. 1, 13–14 (1972).

191 *Clapper*, 568 U.S. at 415–416.

192 *Laird*, 408 U.S. at 13–14.

193 *Clapper*, 568 U.S. at 417–18.

194 *Id.* at 418.

victims will need to demonstrate the government is the right party to go after for redress.[195]

Injury in the context of digital surveillance will likely be more difficult to show than in the mosque infiltration context because digital surveillance often occurs undetected.[196] Whereas in the infiltration context, congregants became suspicious of outsiders who had suddenly appeared in the community and began asking invasive questions and then altered their religious practice because of it, in the digital context, surveillance can occur in multiple spaces at the same time, without confinement to a certain house of worship or local community.[197] A court will likely rule against challengers if they simply claim they changed their practices because of subjective fear that they were surveilled.[198] Unlike in the mosque infiltration context, they will likely have difficulty pointing to specific individuals who, for example, started asking suspicious questions.[199]

One may overcome this hurdle by demonstrating that rather than a subjective chill, there is actually a specific, objective present or future threat of harm. To do this, challengers must once again creatively frame the action. *Hassan* recognized an injury because it found the discriminatory classification was an injury and distinguished this from *Laird*, where the Court found no injury.[200] Challengers in the digital surveillance space can likewise argue that targeting Muslim apps or Muslim social media users is similarly a discriminatory classification based on religion. They can distinguish their case from opinions where the Court found no standing by emphasizing that in those cases

---

195 *Id.* at 409.

196 *See, e.g.*, Shankland, *supra* note 59 (describing how users can secretly install Pegasus and spy).

197 *See, e.g.*, Umar A. Farooq, *How an FBI Informant Destroyed the Fabric of an Entire Community*, MIDDLE E. EYE (Nov. 9, 2021, 6:59 PM), https://www.middleeasteye.net/news/fbi-surveillance-of-california-mosques-destroyed-fabric-community (describing how an FBI informant "was relentless in pushing questions about violence").

198 *See Clapper*, 568 U.S. at 416 ("Respondents' contention that they have standing because they incurred certain costs as a reasonable reaction to a risk of harm is unavailing—because the harm respondents seek to avoid is not certainly impending. In other words, respondents cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending.").

199 *See* Farooq, *supra* note 197.

200 *See* Hassan v. City of New York, 804 F.3d 277, 290–91 (3d Cir. 2015).

there was nondiscriminatory government surveillance, whereas here, the government targets religious minorities.[201]

The favorable outcomes in *Hassan* and *Raza* can also help future challengers demonstrate causation and redressability. Opponents may argue modern society is becoming more and more digitized with apps collecting information for various reasons and, because of digitization, it may be difficult to show a certain practice caused an injury compared to physical surveillance where there is concrete evidence. This point is counterintuitive, however, because challengers can also use sophisticated technology to trace specific practices. For example, watchdog groups like Amnesty International tracked the use of Pegasus precisely because they had their own access to sophisticated technology to do so.[202]

The settlement of the mosque infiltration cases also demonstrates redressability is possible, at least with respect to payment of damages.[203] A more cynical theory may be that it was redress of mosque infiltration that caused law enforcement to turn to even more covert tactics, like digital surveillance.

The difficulty in demonstrating standing with digital surveillance suggests law enforcement and national security agencies are more likely to turn to these technologies because of the ease and lack of accountability.[204] On the other hand, the focus of advocacy groups on digital technology and the increasing coverage in media combined with the Court's recent invigoration of the free exercise doctrine suggests courts may be more receptive to such arguments.[205]

---

[201] *Compare Clapper*, 568 U.S. at 403 ("[T]he FISC issued orders authorizing the Government to target international communications into or out of the United States . . . ."), *with* Cox, *supra note* 1 (explaining Muslim Pro is a Muslim lifestyle app serving predominantly Muslim users).

[202] *See, e.g.*, FORENSIC METHODOLOGY REPORT, *supra* note 98, at 6; Scott-Railton et al., *supra* note 99.

[203] *See Hassan v. City of New York*, *supra* note 171.

[204] *See, e.g.*, Faiza Patel, *The Costs of 9/11's Suspicionless Surveillance: Suppressing Communities of Color and Political Dissent*, BRENNAN CTR. FOR JUST. (Sept. 8. 2021), https://www.brennancenter.org/our-work/analysis-opinion/costs-911s-suspicionless-surveillance-suppressing-communities-color-and ("The FBI, [Department of Homeland Security], and local police have spied on the Black Lives Matter movement, immigration activists, and environmental campaigners [using social media].").

[205] *See id.*; Kennedy v. Bremerton Sch. Dist., 142 S. Ct. 2407, 2415–16 (2022) (upholding a coach's right to offer a personal prayer on the field following a football game).

3. Demonstrating a Chilling Impact

Levinson-Waldman advises that to demonstrate chilling, "victims . . . can point to concrete ways that it prevented them from exercising their First Amendment rights—for instance, if they pulled back on political organizing, activism, or communications."[206] Government actions like those taken in the Muslim Pro Case, potentially taken using Pegasus, and social media mining are chilling religious exercise, and victims are changing their practices.[207] This threat of chilling is not simply theoretical but reported.[208] A clear example is the behavior of social media users. Professors Aziz and Khaled Beydoun describe what they call the "spiral-of-silence effect."[209] Although they caution that understanding the chilling impact of online government surveillance requires further analysis, their research combines existing empirical studies on social media users' behavior after being told the government monitored them, with research on Muslims experiencing surveillance to argue that there are increased risks to Muslims' protected First Amendment activities.[210] A 2016 study on social media users showed that users were less likely to post content they believed observers would disagree with, and they became significantly less likely to speak out on social media when told the government was surveilling them.[211] The fact "[t]hat online expressions of opinion leave digital footprints traceable years later further exacerbates the spiral-of-silence effect."[212] While these studies may initially appear to only implicate free speech in the ordinary sense—refraining from saying things—when looked at through an Islamic tradition they also say plenty about implications for free exercise.

A large part of practice in Islam is *Dawah*, the act of inviting people to the Islamic faith.[213] While it includes what Muslims say, it also implicates how they interact or share their faith with others.[214]

---

206 Levinson-Waldman, *supra* note 71, at 540.

207 Aziz & Beydoun, *supra* note 65, at 1177.

208 *Id.*

209 *Id.*

210 *Id.*

211 Elizabeth Stoycheff, *Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring*, 93 JOURNALISM & MASS COMMC'N Q. 296, 303–04 (2016), https://doi.org/10.1177/1077699016630255.

212 Aziz & Beydoun, *supra* note 65, at 1177.

213 *See* Ahmad Ansari, *Divine Methodology of Dawah*, ISLAMICITY (Aug. 5, 2023), https://www.islamicity.org/3143/divine-methodology-of-dawah.

214 *Id.*

Dawah is central to religious practice—in fact, it is an obligation upon every individual Muslim, not just religious leaders.[215] It is not only how Muslims portray Islam—it also concerns addressing any misunderstandings or misperceptions of the religion.[216] In the Quran, Allah commands Prophet Muhammad (PBUH) to "invite to the way of your Lord with wisdom and good instruction, and argue with them in a way that is best."[217] Thus, because of *Dawah*, government surveillance that explicitly implicates speech has the potential to uniquely chill Muslims' free exercise.[218]

It is important to note, however, that the courts and literature have not yet fully explored the implications for religious practice.[219] This may be because of the inherent secrecy.[220] This is in striking contrast to the Fourth Amendment doctrine, particularly in the social media spying context.[221] Perhaps another explanation is that Fourth Amendment issues are more concrete, at least in the sense that they do not depend on individual practices, like religious exercise does, which is both very personal and individualized to each worshipper. Despite this, it is important not to lose sight of the religious freedom implications of this government conduct because religious freedom intersects with so many other civil liberties.[222] The unique intersection of speech and free exercise in *Dawah* is one such example.[223] This intersection is particularly important for another reason, as it may be a hybrid route to challenge free exercise restrictions as the Court alluded to in *Smith*.[224]

---

[215] *Id.*

[216] *Id.* For example, Muslims utilize social media to debunk Islamophobia. *See* Aziz & Beydoun, *supra* note 65, at 1164–65.

[217] Quran 16:125.

[218] *See, e.g.*, Farooq, *supra* note 197 (describing how Muslim community members assigned to help a new convert learn the religion began restricting both their religious speech and practice, like attending the mosque, once they became suspicious that a member was an undercover FBI informant).

[219] *See* Aziz & Beydoun, *supra* note 65, at 1177 (cautioning that understanding the chilling impact of online government surveillance requires further research).

[220] *See* Cox, *supra* note 1 (reporting how the US government bought Muslim users' location data secretly).

[221] *See* Aziz & Beydoun, *supra* note 65, at 1153; Simchi-Levi, *supra* note 69, at 997; Jones, *supra* note 70, at 69–70; Levinson-Waldman, *supra* note 71, at 525.

[222] *See* S. REP. NO. 94-755, at 290 (1976) (reporting how government spying implicated a multitude of First Amendment rights).

[223] *See, e.g.*, Ansari, *supra* note 213.

[224] *See* Emp. Div. v. Smith, 494 U.S. 872, 881–82 (1990).

Digital surveillance also very likely has repercussions for another major tenet of Islam: *Zakat*, obligatory, annual charitable giving, based on a pattern of law enforcement practice. During the mosque infiltration period, the government took a particular interest in Muslim charities and donors, thereby causing a chilling effect on those surveilled as they stopped giving to avoid suspicion and surveillance.[225] As charitable giving has transitioned online with options to donate to a wider range of organizations, causes, and geographic regions, there is a high possibility that digital surveillance will chill this religious practice as well.[226]

4. Counterarguments to First Amendment Application

The only argument the government ever makes to justify surveillance, be it physical infiltration or digital, is national security. The government made this assertion in 2001 in the mosque infiltration context and continues to do so in the context of digital surveillance, with the government often refusing to cooperate with requests for more information citing national security concerns.[227] National security drives conversations because of the traditional deference to government and law enforcement in this area. Is surveillance a necessary evil to protect national security, or is that justification a pretext to continue policing unpopular groups? One thing is true: government surveillance targets people often without any suspicion,[228] which creates a cycle through which those targeted individuals become guilty simply by association with a government investigation.[229]

The big problem in answering this question is that the public is often told the specific national security justifications are confidential, and sometimes those very same justifications are incorrect, exaggerated, or misguided. Iraq is the prime example of erroneous

---

225 *See, e.g.*, BLOCKING FAITH, FREEZING CHARITY, *supra* note 38, at 9.

226 *See, e.g.*, Stoddard, *supra* note 123 (explaining that Muslims stopped donating as much when government targeted Muslim charities following September 11).

227 *See Hassan v. City of New York*, *supra* note 171; Rafei, *supra* note 37 ("The FBI attempted to stop the litigation of the plaintiffs' religious discrimination claims by arguing that further proceedings could reveal state secrets.").

228 *See Hassan v. City of New York*, *supra* note 171.

229 Farooq, *supra* note 197 (detailing how a Muslim man, who reported an FBI informant to the Council on American-Islamic Relations (CAIR), was still investigated and publicly named a terrorist suspect, after which his social circle distanced themselves from him, forever damaging his relationships).

information provided to justify US invasion.[230] Many more exist.[231] There is a clear tension between national security and First Amendment rights, with marginalized communities often facing the brunt of this tension. Ultimately, "[t]he critical need to ferret out terrorism cannot be allowed to collapse the necessary tension between First Amendment freedoms and protecting the national security."[232] Even though such a tension exists, it is not new. After all, the United States ratified the First Amendment following, arguably, the earliest national security threat in American history—the Revolutionary War. This implies the framers were aware of this tension and crafted the First Amendment precisely to protect those who may be most vulnerable during a national crisis.[233] Because of this, society must be aware of when such national security justification is given and against whom.[234] If the generational trauma of Muslims and other communities shows anything, it is that the human toll is chilling.

V. WHERE TO GO FROM HERE?

A. *Solutions*

The ultimate question is how Americans should grapple with increasingly sophisticated, secret surveillance. Perhaps there is no one right answer. Technology has allowed the world to achieve feats thought to be impossible a few years ago. At the same time, when

---

[230] *See generally* Press Release, U.S. Senate Select Comm. on Intel., Senate Intelligence Committee Unveils Final Phase II Reports on Prewar Iraq Intelligence (June 5, 2008), https://www.intelligence.senate.gov/press/senate-intelligence-committee-unveils-final-phase-ii-reports-prewar-iraq-intelligence (listing the Bush Administration's erroneous statements on prewar Iraq).

[231] *See, e.g.*, Neal Katyal, *Confession of Error: The Solicitor General's Mistakes During the Japanese-American Internment Cases*, THE JUST. BLOG (May 20, 2011), https://www.justice.gov/archives/opa/blog/confession-error-solicitor-generals-mistakes-during-japanese-american-internment-cases (confessing that the government presented false evidence to the Supreme Court during the internment of Japanese Americans).

[232] Linda E. Fisher, *Guilt by Expressive Association: Political Profiling, Surveillance and the Privacy of Groups*, 46 ARIZ. L. REV. 621, 641 (2004).

[233] *See, e.g.*, Aldir Guedes Soriano, *Liberal Democracy and the Right to Religious Freedom*, 2013 BYU L. REV. 581, 588–89 (2013) ("[T]he [main] purpose of the democratic . . . state is to protect the human person and [their] unalienable rights. . . . [T]he state can neither revoke nor restrict human rights at its own pleasure because it was not the author of those rights." (emphasis removed)).

[234] *See* Patrick Toomey & Ashley Gorski, *The Privacy Lesson of 9/11: Mass Surveillance Is Not the Way Forward*, ACLU (Sept. 7, 2021), https://www.aclu.org/news/national-security/the-privacy-lesson-of-9-11-mass-surveillance-is-not-the-way-forward.

abused, it has caused generational trauma to vulnerable communities.[235] Perhaps there are also no litigation or legislation solutions to protect religious liberty against government surveillance. As *Hassan* and *Raza* demonstrate, litigation is costly in both time and money. It often results in settlements, which have the potential to address current issues but not new issues once advanced technology is developed. Legislation might be even more problematic. The politicized nature of the legislative branch has all but ensured comprehensive legislation aimed at addressing this issue will likely fail or be extremely weak due to the need to compromise to pass legislation.[236] But litigation and legislation efforts are key for a number of other reasons, particularly litigation. Litigation is instrumental to pushing back against surveillance, raising consciousness, and forcing the government to explain, at least partly, its actions to the public.

The ultimate solution may be to lean into First Amendment protections rather than lean out, especially with the Court's focus on religious liberty recently.[237] After all, it was the freedom of the press that uncovered the program Muslims in New York and New Jersey always suspected.[238] It was also active journalism that exposed the sale of Muslim Pro data to the government.[239] Finally, it was a human rights organization that tracked the use of Pegasus against activists and dissidents.[240] The freedoms of religion, press, speech, and association are mutually reinforcing.[241] When one is threatened, others may be threatened too, but those others can be used to defend the threatened right. When action threatens freedom of religion, it is the work of activists, lawyers, and journalists that challenges such action and brings

---

[235] Professors Aziz and Beydoun describe how "the longstanding history of surveillance" has followed vulnerable groups, like Black and Muslim communities, online, which can cause anxiety, fear, and danger. *See* Aziz and Beydoun, *supra* note 65, at 1190–91; Khan & Ramachandran, *supra* note 39.

[236] *See, e.g.*, *Good Question: Why Is It So Hard to Pass a Law?*, CBS NEWS MINN. (June 23, 2016, 10:56 PM), https://www.cbsnews.com/minnesota/news/good-question-passing-bills.

[237] *See, e.g.*, Kennedy v. Bremerton Sch. Dist., 142 S. Ct. 2407, 2415–16 (2022) (holding the school violated a coach's free exercise rights).

[238] Hawley, *supra* note 45.

[239] Cox, *supra* note 1.

[240] FORENSIC METHODOLOGY REPORT, *supra* note 98, at 6.

[241] *See generally* Press Release, United Nations Human Rights, Use Human Rights Frameworks to Promote Freedoms of Religion, Belief, and Expression: UN Experts (Mar. 6, 2023), https://www.ohchr.org/en/press-releases/2023/03/use-human-rights-frameworks-promote-freedoms-religion-belief-and-expression.

attention to it. Challenging government practices, although not always an immediate success, helps develop doctrine and leads to the creation of watchdog groups. If the government is watching, the world should be watching too.

When law enforcement threatens such rights as free exercise of religion, the best way to challenge that threat is to not only rely on existing free exercise jurisprudence but also on other rights like freedom of press that help challengers document the chilling effect of such law enforcement action. After all, the greatest threat to civil liberties is not government abuse of such liberties or even government surveillance. Rather, the greatest threat is the fear of such surveillance that paralyzes individuals and stops them from using such rights to challenge government action in the first place.

B. *Democracies and Surveillance*

A fundamental question is whether surveillance and "democracy" can coexist in the first place. Is a government that spies on its citizens upholding liberty and justice for all, or is it impermissibly violating their rights? Perhaps the key question is not whether surveillance can exist in a democracy but to what extent society will accept it and against whom. The ramifications of government surveillance using sophisticated digital tools are particularly severe in an increasingly globalized world where communications occur almost exclusively in the digital realm. It is a serious blow to civil liberties "when the state seeks to learn what people are reading, thinking, and saying privately."[242] Not only does government surveillance implicate civil liberties, but it also causes sociological and psychological impacts: "many forms of surveillance—covert and overt, public and private—menace our intellectual privacy and the processes of belief formation on which a free society depends. They also create a power imbalance between the watcher and the watched that creates risks of blackmail, undue persuasion, and discrimination."[243]

Digital surveillance poses unique risks for religious minorities. "[It] is more threatening for over-policed groups, like Black or Muslim communities, whose collected data is frequently resold to government agencies for the purpose of surveilling them."[244] This brings up particular concerns about the future of pluralistic democracy. Can

---

[242] Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1951 (2013).

[243] *Id.* at 1962.

[244] Beydoun, *supra* note 181, at 776.

such a democracy exist if a few groups bare most of the costs of digital surveillance? The Third Circuit in *Hassan* warned against this very notion.[245] The targeting of Muslims does not matter just because it may violate religious freedom today. It also matters because if society blindly accepts this targeting now, the legal implications are one more chip in a history of subjugation and rights abuses that will ultimately cause the image of a pluralistic democracy to tumble altogether while eroding the very civil liberties that created that image. Enforcing First Amendment freedom of religion restraints, one of the first freedoms the framers styled, is essential to pluralistic democracy because such restraints also support the free exchange of ideas, encourage political participation, and preserve individual identity and liberty.[246]

VI. CONCLUSION

Digital surveillance replaces in-person surveillance typically conducted by undercover government informants. Digital surveillance programs like the Muslim Pro Case, Pegasus, or even on social media threaten to infect every crevice of modern-day life, not just houses of worship like the surveillance conducted post-2001. Because digital surveillance is more widespread, its chilling impact on religious liberty and free exercise is unprecedented. While it will be difficult to challenge digital surveillance on the basis of free exercise, as evidenced by the courts' holdings in *Raza* and *Hassan*, a successful challenge is possible. Challengers must be strategic in framing their free exercise claims and anticipating standing barriers. Finally, they will need to demonstrate that such digital surveillance is chilling their daily practice.

Digital surveillance programs are incompatible with a constitutional system that doubly protects religion because they chill individuals' rights to freely exercise that religion. These programs have overcome traditional barriers like the need for traditional law enforcement planning, personnel, time, and money, and have provided the government with the ease and convenience of spying from anywhere in the country. Because of this, digital technology is the future of spying and the greatest threat to individual rights. Society must be vigilant in enforcing freedom of religion restraints in this context and find creative ways to do so because freedom of religion is

---

[245] Hassan v. City of New York, 804 F.3d 277, 309 (3d Cir. 2015).

[246] *See What in the World Is Religious Freedom?*, RELIGIOUS FREEDOM INST. (Nov. 1, 2019), https://religiousfreedominstitute.org/what-in-the-world-is-religious-freedom.

a vessel to other rights, and to protect it, is to reinforce other civil liberties.