Emerging Threats to Privacy and Expression Under the Surveillance State: An Analysis and Proposals for Safeguarding Privacy in an Increasingly Regulated and Digital World

Scott Blackburn[1] & Daniel Woislaw[2]

I. ABSTRACT

We live in an era of mass digital surveillance. Sixty-three percent of Americans believe it is not possible to go through daily life without the government collecting information about them.[3] And for good reason. American's bank accounts, workplaces, charitable activities and cell phones are all within digital reach of the state – often without any legal protection for citizens. And while this explosion of technology has brought with it significant benefits and improvements, traditional privacy jurisprudence has not kept up with the rapid pace of change. There are at once Fourth Amendment concerns as a result of these new tools, and First Amendment concerns due to the significant threat that massive digital surveillance poses both to an individual's privacy and security.

This paper explores how the law has failed to adequately protect privacy and the freedoms of speech, expression, and association in the face of modern surveillance. It examines four categories of surveillance: (1) electronic dragnets, (2) licensing and permitting powers, (3) financial transactions, and (4) donor disclosure requirements. For each category, it explores the legal background that has developed to permit this surveillance and how that body of law has developed (or failed to) alongside changes in technology and expansions in government surveillance and regulation. Each section draws attention to the overlooked harms to free speech, association and other First Amendment rights enabled by the widespread technological innovation that allow a detailed picture of every facet of one's life to be captured by the state. Finally, this paper offers potential legislative and judicial solutions in an attempt to understand how we are to regain some of our lost privacy in this digital world.

A. Surveillance through electronic dragnets

---

[1] Scott Blackburn is a Privacy Scholar with the Libertas Institute. He has worked in policy research for over a decade – studying the First Amendment impacts of campaign finance laws and regulations, disclosure mandates, internet speech rules and other judicial and legislative efforts that affect free speech and association. He was previously the Research Director at the Institute for Free Speech and is currently the Legal Portfolio Manager working on judicial policy at Americans for Prosperity. This paper represents his views and not those of his employer.

[2] Daniel Woislaw is a Privacy Scholar with Libertas Institute and an attorney specializing in constitutional property and privacy law with Pacific Legal Foundation. He holds a J.D magna cum laude from The Antonin Scalia Law School at George Mason University and previously worked as a public defender in Norfolk, Virginia representing indigent juveniles and adults. He is licensed in Virginia and admitted to practice before the U.S. Supreme Court, Virginia Supreme Court, and several U.S. Circuit Courts of Appeal.

[3] Brooke Auxier, et al, *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, Pew Research Center (November 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/

Nowhere has the law lagged further behind the practice and experience of everyday life than in the field of technology, particularly where advancements in computing and electronics are concerned. Although smartphones have been in use since 2007, the U.S. Supreme Court took until 2014 to confirm that a warrant is needed for the police to search the contents of a cell phone, even after a suspect is arrested with one in his possession.[4] But technological advancements today have far outstripped the capabilities of the first iPhone. Today, a surveillance plane can circle a city, cataloguing the movements of its inhabitants with startling detail.[5] Facial recognition software can pick individuals out of a crowd with ease.[6] License-plate readers on police cars and mounted over highways can catalogue people's movements and analyze patterns in their behaviors.[7] Even the passive location data generated from a person's cell phone refreshing their email inbox and generating notifications can allow someone with access to that data to reconstruct the intimate details of the owner's life.[8]

Data mining and marketing companies are buying troves of user data from technology companies and websites that track or catalogue the activities of their users. Even after such data is anonymized, it is often not difficult to find out to whom a particular piece of data belongs.[9] And government agencies, in an end-run around recent constitutional court rulings,[10] have been *purchasing* it.[11]

There is no silver-bullet policy solution to protect Americans from the intrusive government surveillance these advancements make possible. But recourse to the courts alone has thus far proven a limited option for relief. The lack of updated privacy jurisprudence coupled with the slow-moving nature of the courts has created a massive problem.

Consider the language of the Fourth Amendment, which protects only "persons, houses, papers, and effects" from "unreasonable searches and seizures."[12] Can it be said that a camera merely recording someone's face as they walk by is engaging in a "search?" What about when that camera is equipped to scan and recognize faces and then link those faces to information from a database?

---

[4] Riley v. California, 573 U.S. 373 (2014).

[5] See Leaders of a Beautiful Struggle v. City of Baltimore, 2 F.4th 330 (4th Cir. 2021).

[6] Paul Mozur, *Inside China's Dystopian Dreams: A.I., Shame and Lots of Cameras*, N.Y. TIMES (July 8, 2018), https://www.nytimes.com/2018/07/08/business/china-surveillance-technology.html.

[7] Thomas Brewster, *This AI Watches Millions of Cars and Tells Cops if You're Driving Like a Criminal*, FORBES (June 17, 2023 06:30 AM EDT), https://www.forbes.com/sites/thomasbrewster/2023/07/17/license-plate-reader-ai-criminal/?sh=58dfc4573ccc.

[8] See Carpenter v. United States, 585 U.S. 296, 310 (2018) (citing United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring) ("As with GPS information, the time-stamped data provides an intimate window into a person's life, revealing not only his particular movements, but through them his 'familial, political, professional, religious, and sexual associations.').

[9] See generally Amicus Brief of Data Privacy Experts, Alabama v. U.S. Dept. of Commerce, No. 3:21-CV-211-RAH (M.D. Ala. Apr. 23, 2021).

[10] *Carpenter*, 585 U.S. at 318–20 (ruling government could not subpoena cell-site-location information without a warrant).

[11] Kevin Collier, *U.S. government buys data on Americans with little oversight, report finds*, NBC NEWS (June 13, 2023), https://www.nbcnews.com/tech/security/us-government-buys-data-americans-little-oversight-report-finds-rcna89035.

[12] U.S. Const. amend. IV.

Some scholars have argued that people have a "reasonable expectation of privacy" against this type of surveillance under the Fourth Amendment even when they travel in a public space and therefore facial recognition is a search that should require a warrant based on probable cause:

> In walking down the street, we invite "the intruding eye" of strangers to glance at or even examine our faces as we pass by, but we do not invite them to also identify us by our names and addresses, much less occupation, immigration status, criminal history, and other personal information. … In many places, we expect to be able to take trips to the pharmacy to purchase sensitive items, or private trips to the doctor's office or the therapist's office, or perhaps a quick trip to the grocery store in pajamas, with the minimal risk of being recognized and of being required to identify ourselves in public.[13]

Courts have not uniformly agreed.[14] When it comes to the non-physical invasions of privacy contemplated by the collection and use of digital media, courts ask whether a person has a "reasonable expectation of privacy" in determining whether a surveillance tactic violates the Fourth Amendment. This doctrine, as Justice Scalia cautioned in a 2001 decision by the Supreme Court about the use of a thermal imaging device by the police, "has often been criticized as circular, and hence subjective and unpredictable."[15] More recently, Justice Gorsuch lamented that the expectation-of-privacy test is one "whose contours are left to the judicial imagination."[16] Moreover, the courts have not yet jettisoned another legal rule called the third-party doctrine, which holds that there is no expectation of privacy in information voluntarily shared with a third party (see *Section C - Surveillance through financial transactions*). If one considers how many end-user agreements under which they click "I agree" on a daily basis, this doctrine may severely limit constitutional protections for privacy against digital surveillance where the expectation-of-privacy test controls the outcome. The Supreme Court has provided very little guidance on how (or whether) this third-party doctrine applies to new technologies and the services that go along with them.[17]

However, there are some glimmers of hope in the Court's pivot away from privacy expectations in evaluating Fourth Amendment cases and *toward* property interests. After all, the text of the Amendment lists "persons, houses, papers, and effects" as the items to be "secured" rather than some vague expectation of privacy. And just as freedom of the press under the First Amendment extends beyond physical newspapers churned out by actual presses, including also digital articles, so too does the Fourth Amendment extend beyond physical "papers" to digital ones.

The Framers of the Bill of Rights deliberately included "papers" within the list of property protected against unreasonable searches and seizures under the Fourth Amendment to emphasize

---

[13] Mariko Hirose, *Privacy in Public Spaces: The Reasonable Expectation of Privacy Against the Dragnet Use of Facial Recognition Technology*,

[14] See *United States v. Tuggle*, 4 F.4th 505 (7th Cir. 2021).

[15] *Kyllo v. United States*, 533 U.S. 27, 34 (2001).

[16] *Carpenter*, 585 U.S. at 391 (Gorsuch, J., dissenting).

[17] *Id.* at 405 (Gorsuch, J., dissenting) (describing court's ruling as keeping the third-party doctrine "on life support" where the court ruled the doctrine did not apply to cell-site-location information an owner shared with a telecommunications company by connecting to a cell tower).

the importance of privacy and security in personal documents and records.[18] Several landmark court cases in England around the time of the Founding informed the Framers' thinking.[19] In *Wilkes v. Wood* (1763)[20] and *Entick v. Carrington* (1765),[21] political enemies of the Crown had their houses and papers searched without properly issued judicial warrants for evidence they had authored tracts critical of the government. Freedom of the press, speech, association, and privacy have often intermingled in the struggle for freedom from arbitrary government intrusion and regulation.[22] Indeed, even the Fifth Amendment's right against self-incrimination shares a common nexus. Religious and political opponents of the ruling monarch in England (whose religions and politics changed from generation to generation) were commonly targeted for their publications, practices and beliefs, summoned before a government panel, put to an oath, and ordered to produce and identify the private papers in their possession that, if proven to be theirs, would sentence them to death or life imprisonment.[23]

Private papers, as that term is understood within the context of the Fourth Amendment, includes business records, and by extension documents identifying donors, patients, guests, or clients. As recently as 2015, the Supreme Court held in *City of Los Angeles v. Patel*[24] that a local ordinance violated the Constitution by requiring hotels to allow government inspection of their guest records upon demand.[25] Yet, federal and state courts have often found that businesses engaged in closely regulated industries retain no constitutional privacy interest in their business records, particularly when the records only exist as a result of regulations that require them to be made and retained.[26] This trend has ushered in mandatory, sweeping donor disclosure laws.

While Fourth Amendment jurisprudence has failed to keep up with the speed and scope of mass technological surveillance, the spillover effects of that surveillance now pose a serious First Amendment harm as well. In 2012, Justice Sonia Sotomayor recognized that warrantless GPS tracking "generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations."[27] In the past 20 years that record has become both more detailed and easier to analyze for government officials. If the states of the South in the 1950s had access to the level of technology available to government officials today, there would be no need for the laws requiring membership

---

[18] U.S. Const. amend. IV.

[19] *Boyd v. United States*, 116 U.S. 616, 626–27 (1886) (maintaining that it can be "confidently asserted" that the *Wilkes* case and its results "were in the minds of those who framed the Fourth Amendment").

[20] 98 Eng. Rep. 489 (K.B. 1763).

[21] 19 State Trials 1029, 1073 (K.B. 1765).

[22] Cf. *Marcus v. Search Warrant of Property*, 367 U.S. 717, 724–29 (1961) (outlining the history of the relationship between the struggle for freedom of the press and the scope of the search and seizure power in England).

[23] See generally Leonard Levy, ORIGINS OF THE FIFTH AMENDMENT: THE RIGHT AGAINST SELF-INCRIMINATION (1968) (detailing the history and origins of the right against self-incrimination and its codification in the U.S. Constitution's Fifth Amendment).

[24] 576 U.S. 409 (2015).

[25] *Id.* at 424–25.

[26] See generally Ann K. Wooster, *Validity of Warrantless Administrative Inspection of Business that is Allegedly Closely or Pervasively Regulated*, 182 A.L.R. Fed. 467 (A.L.R. 2002) (updated 2022).

[27] *United States v. Jones*, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring).

lists from civil rights organizations to chill their activity – states could simply collect the cell phone data of a known member of the group and, through that, find an entire connected network.

Recently, government officials have even begun using speech itself as the tool for surveillance. Law enforcement has begun to seek and obtain keyword search warrants concerning data on everyone within a certain geographic area that searched a particular phrase in Google.[28] While the courts have not yet ruled on the details of permissibility and requirements for such searches, the potential for harm to free speech is obvious. Searches like "how to get an abortion out of state," "when's the January 6 Trump protest going to start" and "buy a prescription from a doctor" could suddenly land one in a permanent police database. Current protections rely on outdated Fourth Amendment jurisprudence and the goodwill of technology companies.

The pandemic, and the government's invocation of emergency powers, saw the use of dragnet surveillance extend to previously unimaginable levels. At Calvary Chapel in Santa Clara, California, geolocation cellphone data was collected and sold to the state government. The state then used the data to fine the church pastor for holding illegal service that violated the state's newly-issued rules against large gatherings.[29] No warrants were sought; no probable cause was found – just a direct line from dragnet data collection to law enforcement shutting down the free exercise of religion.

B. Surveillance through the licensing and permitting power

The idea that one's home or business could be searched by the government without a warrant supported by probable cause was anathema to the Founding Fathers. Indeed, the unannounced searches of colonists' properties during British rule was one of the catalysts for the American Revolution itself and, ultimately, the Fourth Amendment of the United States Constitution.[30] Yet today, under the guise of licensing and permitting, the government practice of searching homes and businesses without warrants or suspicion is becoming more commonplace once again.

"Administrative searches" as they are termed by the courts[31] began with comprehensive regulatory schemes that subjected dangerous industrial operations like underground mining[32] to unannounced searches under tightly drawn laws. Now, as more occupations and activities require licenses or permits, these regulatory search powers have proliferated at all levels of government. In America's

---

[28] See Jennifer Lynch & Andrew Crocker, *UPDATE: Colorado Supreme Court Grants Review in First U.S. Case Challenging Dragnet Keyword Warrant*, Electronic Frontier Foundation (June 30, 2022), https://www.eff.org/deeplinks/2022/06/eff-file-amicus-brief-first-us-case-challenging-dragnet-keyword-warrant.

[29] Maggie M. Phillips, *Just the Facts on 'Geofencing,' the Intrusive, App-Based 'Dragnet' That Sgt. Joe Friday Never Dreamed Of*, REALCLEAR INVESTIGATIONS (Sept. 26, 2023 2:55 PM ET), https://www.realclearinvestigations.com/articles/2023/09/26/just_the_facts_on_geofencing_the_intrusive_app-based_dragnet_that_sgt_joe_friday_never_dreamed_of_981539.html

[30] See NELSON B. LASSON, THE HISTORY AND DEVELOPMENT OF THE FOURTH AMENDMENT TO THE UNITED STATES CONSTITUTION 51–78 (1937) (discussing the history of the writs of assistance in the colonies as a contributor to the American Revolution and development of the Fourth Amendment).

[31] See *City of Los Angeles v. Patel*, 576 U.S. 409, 420 (2015) (recognizing "administrative searches" as those motivated by "special needs" other than criminal law enforcement that render the warrant process unworkable).

[32] See 30 U.S.C. § 813(a) (1977) (providing for unannounced inspections of "coal or other mines"), *amended* 2006; see also Donovan v. Dewey, 452 U.S. 594, 605 (1981) (upholding the Act).

increasingly regulated society, licensing and permitting have become significant threats to Americans' privacy and associational freedoms as new regulations increasingly require applicants for benefits, licenses, and permits to surrender their right to demand a warrant before their homes, businesses, records, and even their persons can be searched, often without any suspicion much less probable cause.

The number of activities for which Americans must obtain government permission increases with each passing year. In the 1960's, roughly 1 in 20 occupations required a license.[33] Today, that number is closer to 1 in 4.[34] This number does not include recreational licenses, like those required to hunt, fish, boat, or host an event. Nor does it include transactional licenses, like building permits (often required for even minor improvements). While the cost in time and expense of acquiring the necessary permits and licenses pose significant problems, the surrender of privacy and property rights should not be overlooked.

Resisting the administrative inspections that go along with so many licenses and permits today can quickly become expensive. One licensing scheme for short-term vacation rentals near Lake Placid, New York imposed fines of up to $3,000 per week for each week a property owner continued in their refusal of an unannounced search of their home.[35] Many schemes even impose criminal punishments for refusing a warrantless search. In Ohio, practicing taxidermy could open a person's house to unannounced searches under the risk of criminal prosecution for demanding a warrant.[36] Under federal law, the same is true for falconers.[37] In Kansas, dog trainers are subject to a similar law.[38] In Billings, Montana, therapeutic massage practitioners must open their properties and treatment logs to inspection or face criminal prosecution.[39] And sea fishermen around the country

---

[33] Executive Summary, The National Occupational Licensing Database, Nat'l Conf. of State Legislatures (Updated Aug. 12, 2022), *available at* https://www.ncsl.org/labor-and-employment/the-national-occupational-licensing-database#:~:text=Over%20the%20last%2060%20years,almost%201%2Din%2D4 ("Over the last 60 years, the number of jobs requiring an occupational license, or government approval to practice a profession, has grown from about 1-in-20 to almost 1-in-4.").

[34] *Id.*

[35] See *Calvey v. Town Bd. of North Elba*, No. 8:20-CV-711 (TJM/CFH), 2021 WL 1146283, at *3 (N.D.N.Y. Mar. 25, 2021) (quoting ordinance).

[36] Andrew Wimer, *Small business owner threatened with jail for refusing warrantless search*, FORBES (Nov. 30, 2021 08:48 AM EST), *available at* https://www.forbes.com/sites/instituteforjustice/2021/11/30/small-business-owner-threatened-with-jail-for-refusing-warrantless-search/?sh=2ccd8afd6c26. This regulation has since been withdrawn by the Ohio Department of Natural Resources. Order, Inspection of Non-Licensed Entity Policy, Division of Wildlife, ODNR (Jan. 4, 2022), *available at* https://ij.org/wp-content/uploads/2022/01/ODNRpolicydirective.pdf.

[37] See 50 C.F.R. § 21.82; see also Scott Shackford, *The government says falconers have to give up their privacy and free speech rights in order to own birds. Now the falconers are suing.*, Reason (Nov. 16, 2018), *available at* https://reason.com/2018/11/16/the-government-says-falconers-have-to-gi/.

[38] See *Johnson v. Smith*, __ F. Supp. __, No. 2:22-CV-1243, 2023 WL 3275782 (D. Kan. May 5, 2023), *appeal filed*, No. 23-3091 (10th Cir. May 19, 2023).

[39] See Ordinance 21-5757, City of Billings, Montana (Apr. 26, 2021), *available at* https://www.billingsmt.gov/DocumentCenter/View/44404/ORD-21-5757-Regulating-Massage-and-Spa-Facilities#:~:text=AN%20ORDINANCE%20OF%20THE%20CITY,ACTION%20AND%20PROVIDING%20FOR%20CRIMINAL

must provide room and board on their boats for federal "catch monitors" who report to the government on the owners' activities.[40]

Without a fix, bureaucrats will continue forcing people to surrender their right to privacy in exchange for their livelihoods, property improvements, recreational interests and hobbies. Currently, there is a patchwork of constitutional litigation around the country on this issue, sometimes involving the Fourth and First Amendments, and other times the Fourteenth. Results in the courts have been mixed and narrow. For example, one federal court ruled warrantless searches of barber shops reasonable,[41] while another ruled administrative searches of medical clinics illegal.[42] Federal and state courts have disagreed with one another about whether particular activities subject their participants legally to unannounced searches. Still others have disagreed about how narrowly or broadly to define an "industry" or activity when deciding whether it is subject to reasonable unannounced searches without warrants.[43]

State-level legislation is uniquely suited to reigning in the power of bureaucrats who demand and exercise these intrusions on Americans' properties and privacy. The response by the courts has been scattered and guidance for regulators and regulatees alike is therefore unclear as to when unannounced search powers comply with the Constitution. The Supreme Court itself has only affirmed the industries of firearms distribution, liquors, underground mining, and automotive scrap-yards as subject to reasonable warrantless administrative searches while striking down an unannounced search law targeted at hotels and another regulation that authorized OSHA to perform unannounced searches in employee-only areas of all regulated businesses. It could be many years before the U.S. Supreme Court clears up its confusing guidance on whether and when unannounced searches imposed as a condition of licensing or permitting regulations comply with the Fourth Amendment.

While this massive expansion of modern licensing regimes and the warrantless searches they authorize is most obviously viewed as a violation of the Fourth Amendment, the sheer size and scope of these regimes also endanger First Amendment rights. Size greatly increases the number of people subject to government intervention. The likelihood of chilling speech or association when the only private space open to warrantless searches were dangerous mine shafts is relatively low; however, individuals maintain private space for private membership and private expression at their homes and hunting clubs and barbershops. But when the warrantless search also applies to one's hunting club because of gun licensure and one's barbershop because of beautician licensure and even one's home because of in-home business or homeschooling licensure then it's only prudent for people to limit what they say and write and with whom they associate.

---

[40] See 50 C.F.R. § 622.204.

[41] *Stogner v. Kentucky*, 638 F. Supp. 1, 3 (W.D. Kentucky Feb. 2, 1985).

[42] *Zadeh v. Robinson*, 928 F.3d 457, 465–66 (5th Cir. 2019).

[43] *Compare* Calzone v. Olson, 931 F.3d 722, 725–26 (8th Cir. 2019) (ruling owner of dump truck used locally for private owner's cattle ranch was engaged in broad industry of commercial truck driving, subjecting him to unannounced stops without suspicion on the highways), *with* Mexican Gulf Fishing Co. v. U.S. Dept. of Commerce, 60 F.4th 956, 968–69 (5th Cir. 2023) (cautioning that "federal courts must not define the industry at issue at too high a level of generality" and proceeding to distinguish between commercial fishing and charter fishing).

This expansion is coupled with the opportunity for pretextual searches by authorities. When a local reporter writes articles critical of the police department, warrantless searches provide an opportunity to harass that reporter if they own a dog or their sister owns a massage parlor. While the reporter would likely win in court, having to put up with the illegal search, face targeted harassment and then the cost in time and money of challenging the massive regulatory apparatus with its veneer of acceptability is enough to deter nearly anyone. The process is the punishment.

Further, licensure regimes blur the line between public and private spaces. This also adds an additional layer of First Amendment harm – fear of mistaken association. By exposing all massage therapy businesses, for instance, to potential search instead of targeting those suspected of illegal activity through warrants, the state has assigned to the industry writ-large an imprimatur of criminality. Now, an individual may reasonably be wary of doing business with legitimate enterprises for fear that that association is catalogued in a government search or database. This threat is further enhanced in the modern era of government surveillance, where technology allows police to easily maintain and easily access the nearly limitless data it obtains in warrantless searches and recordkeeping requirements (for more, see *Section A. Surveillance through electronic dragnets*).

C. Surveillance through financial transactions

The story of financial transaction surveillance, like many stories about the erosion of American constitutional rights, begins with Richard Nixon. In response to the perceived use of foreign bank accounts as a vehicle for tax evasion, Nixon signed into law the Bank Secrecy Act in 1970.[44] This act radically transformed the financial services industry, but from the view of individual privacy, the most important provision required that financial institutions report certain financial transactions to the U.S. government (at the time only single transactions of $10,000 or more – the equivalent to roughly $77,000 today.).

Lawsuits followed, arguing that these violated the Constitution. The bulk of the arguments against this mandatory reporting of transactions relied on the Fourth Amendment. By mandating that banks collect these records and send them off to the government, the bank, it was argued, was an agent of the state and had improperly seized the records. In *United States v. Miller*,[45] the court disagreed and instead established the third-party doctrine where it stated, "we perceive no legitimate expectation of privacy [in bank records]. The depositor takes the risk in revealing his affairs to another, that the information will be conveyed … to the government."[46]

Not surprisingly, the notion that one would have to choose between Fourth Amendment privacy protections and possessing a bank account caused tremendous consternation among the public, which prompted Congress to attempt taking up the mantle of privacy protection that the Court dropped. Two years after *Miller*, Congress enacted the Right to Financial Privacy Act, which intended to create an avenue for citizens to gain knowledge of and potentially challenge

[44] Bank Secrecy Act of 1970, Pub. L. No. 91-508, 84 Stat. 1114 (1970).
[45] 425 U.S. 435 (1976).
[46] *Id.* at 442–43.

government attempts at financial transaction surveillance.[47] Equally unsurprisingly, however, the Right to Financial Privacy Act was riddled with exceptions and over time these exceptions came to swallow the general rule of informing citizens and providing them with an opportunity for due process. By way of example, the act does not apply to third-party disclosures mandated by the IRS or through the tax system. Given the current size and complexity of the tax code, that exception alone renders the act nearly a dead letter with respect to private financial transactions.[48]

And while privacy protection legislation has languished in disrepair, there has been no shortage of expansions of third-party surveillance programs through the broadening of the definition of the financial institutions that must report; broadening the type, number, and circumstances in which a financial institution has to report; increasing the number of agencies that request or mandate these type of disclosures; and, lowering the monetary threshold for when surveillance is required.[49] Most recently, the IRS proposed a rule mandating the reporting for all transactions over just $600,[50] a far cry from the narrow $10,000 threshold whose constitutional blessing by the Court began the era of financial transaction surveillance.

There is an important judicial caveat to this story. The size of the initial third-party disclosures – $10,000 then, the equivalent of $77,000 today[51] – played a significant role in the Court blessing its constitutionality. As Justice Powell wrote in concurrence, "a significant extension of the regulation's reporting requirement ... would pose substantial and difficult constitutional questions for me…financial transactions can reveal much about a person's activities, associations and beliefs. At some point, governmental intrusion … would implicate legitimate expectations of privacy."

Further, the Court brushed aside First Amendment arguments as "premature"[52] since the government of the 1970s had not sought disclosures that would directly infringe on membership and contributor information the way Alabama had in *NAACP.* But given the newly expansive realm that these disclosures now reveal, and the technological ease with which they can be connected to association, it is beyond time to reconsider the First Amendment harms of these rules.

Financial transaction surveillance carries with it many of the harms associated with donor disclosure – namely it can be used as a tool to stifle association with controversial groups and causes by exposing their supporters either to direct governmental reprisal or, as a result of data leaks, to third-party pressure from their political enemies. It likewise carries many of the dangers associated with electronic dragnet surveillance - a person's purchasing behavior, just like their location data, can reveal a great deal of personal information about a person, including their

---

[47] Right to Financial Privacy Act, Pub. L. No. 95-630, 92 Stat. 3641 (1978).

[48] For a more complete history of the Right to Financial Privacy Act, see Nicholas Anthony, THE RIGHT TO FINANCIAL PRIVACY: CRAFTING A BETTER FRAMEWORK FOR FINANCIAL PRIVACY IN THE DIGITAL AGE (Cato Institute Oct. 14, 2022), *available at* https://www.cato.org/sites/cato.org/files/2022-10/working-paper-69.pdf.

[49] See Bank Secrecy Act Timeline 1970-Present, Financial Crimes Enforcement Network, *available at* https://www.fincen.gov/resources/statutes-and-regulations/bank-secrecy-act/bsa-timeline

[50] Implementation of this rule has been delayed to 2023.

[51] Data adjusted for inflation using: "CPI Inflation Calculator," U.S. Bureau of Labor Statistics. Retrieved on September 28, 2023 from Available at: https://www.bls.gov/data/inflation_calculator.htm.

[52] *California Bankers Assn. v. Schultz*, 416 U.S. 21 (1974).

religion, fitness habits, whether they own a dog, or how often they visit particular family members or friends.

But financial transactions offer an even more serious harm to speech and association – if a government finds your speech dangerous, offensive, or unacceptable, it can turn off your bank account. Such was the dire situation in Canada in 2022. When protestors in the Freedom Convoy converged on Ottawa to voice their opposition to government lockdown and vaccination measures, the Canadian government worked with financial institutions to identify and freeze the accounts of protestors.[53] Relying on Canadian disclosure rules that were intended to fight terrorism, the Canadian government deliberately and purposefully attempted to shut down what they viewed as an illegal protest by starving it of financial resources. The Canadian government knew that one's willingness to protest the government, decreases dramatically if the protester can no longer buy groceries for their family.

And while the expansive disclosure laws are the base ingredients that make these substantial free speech harms possible, technological innovations in how we use, store and share money are the catalysts that have propelled this threat to previously unforeseen levels. As Chrystia Freeland said when enacting these anti-protest freezes, "We now have the tools to follow the money, we can see what is happening and what is being planned in real time."[54] Government financial surveillance could identify donors on crowdfunding sites like GoFundMe, it could link names and transactions across accounts and payment platforms, and it could effectively map where and with whom a speaker was spending their money. None of these substantial privacy concerns or their implications on free association were realistically imagined in the 1970s.

These threats are not stopping at the Canadian border. In a case that will come before the Supreme Court in 2024, the state of New York threatened regulatory action against banks that continued to hold accounts with gun rights organizations, while secretly offering leniency to banks that did drop gun rights advocacy groups.[55] Why? New York authorities disagreed with the political and policy positions of the gun rights groups. And after the Capitol riots on January 6, Federal investigators encouraged banks to use explicitly political terms like "Trump" and "MAGA" to help law enforcement identify transactions that they thought could potentially be criminal.[56] Regardless of where you stand on policy on politics, it is clear from these examples that First Amendment activity and one's bank account are more intertwined than ever before.

These technological capabilities also work in tandem with severely lower thresholds (like the IRS $600 rule) as deterrents to speech and association. It currently remains uncertain the extent to

---

[53] Aya Elamroussi et al., *Canadian authorities freeze financial assets for those involved in ongoing protests in Ottawa*, CNN (Feb. 20, 2022 8:48 PM EST), https://www.cnn.com/2022/02/20/americas/canada-trucker-protest-covid-sunday/index.html.

[54] The Canadian Press, *Freeland says some protesters' bank accounts frozen*, YOUTUBE.COM (Feb. 18, 2022), https://www.youtube.com/watch?v=_4I9Rz_g6pU.

[55] See NRA v. Vullo, 49 F.4th 700 (2d Cir. 2022), *certiorari granted*, 144 S.Ct 375 (Nov. 3, 2023)

[56] https://www.foxnews.com/politics/feds-suggested-banks-search-transactions-terms-like-biden-antifa-more-after-jan-6-source

which the popular money transfer app Venmo is required by law to report financial transactions.[57] That is in part because Venmo voluntarily provides government officials information, "where the disclosure of personal information is reasonably necessary to prevent physical harm or financial loss, to report suspected illegal activity, or to investigate violations of the Venmo User Agreement."[58] Venmo also requires that every transaction be accompanied with speech – a brief memo, describing the purpose of the transaction. While 99% of these memo lines are no doubt innocuous, surely some of those messages are provocative, incriminating, personally damaging, or otherwise not fit for public consumption. Thus, Venmo has a database of billions of individual's words detailing each of their financial transactions on the platform – and will cede that data on your speech and association to the government when they arbitrarily decide it is "reasonably necessary."

While it is not currently the case, imagine a world in which Venmo is required to send their 500 million daily transactions to an FBI computer, where the memo line is examined to flag potential illegal or harmful activity. The opportunity for government suppression of dissent and for crackdowns on unwanted association would increase to previously unimagined levels. Given the trajectory of expansive financial surveillance and innovative financial technologies, that world is near.

This is a matter of paramount concern in the digital age. Overly intrusive surveillance not only jeopardizes individual privacy but also threatens the fundamental rights to engage in open discourse and associate freely with others. The mere perception that one's financial activities are constantly monitored can discourage individuals from donating to causes they believe in or participating in social and political organizations. In a society that cherishes the right to express dissenting views and engage in robust debates, safeguarding privacy in minor financial transactions is vital to preserving our democratic values and the integrity of civic engagement.

D. Surveillance through donor disclosure requirements

Donor disclosure encompasses any government collection of records that requires an organization to register and report its supporters publicly or to an agency or government database. Some disclosure laws, like most imposed on political committees and other expressly political groups, require that the database of disclosed information be made public. Others, like those affecting nonprofit organizations and charities, require only that the information be reported to specific government officials. All of them share a common defect: As a condition for engaging in constitutionally protected speech and association, the government is permitted to keep track of an organization's supporters.

Unlike many areas of the law where government surveillance is viewed first through the prism of the Fourth Amendment's prohibition on unreasonable searches and seizures, challenges to laws authorizing government intrusions into records concerning an organization's supporters and donors had the ignominious history of being developed precisely for their chilling effects on political speech and association.

---

[57] See Madison Thompson, *Money Transmitters Face Ambiguity In State, Federal Law*, LEXOLOGY (Dec. 4, 2018), https://www.lexology.com/library/detail.aspx?g=662f9314-4154-49f7-ab8e-39c321450d39.

[58] Venmo Privacy Statement, VENMO (LS Updated Sept. 12, 2023), https://venmo.com/legal/us-privacy-policy/

In the 1950s, in the midst of the Civil Rights Movement, Alabama attempted to force the NAACP to provide the state with a list of its members' names and home addresses. In a unanimous opinion, the Supreme Court struck down the law, saying, "It is hardly a novel perception that compelled disclosure of affiliation with groups engaged in advocacy may constitute as effective a restraint on freedom of association as [other] forms of governmental action."[59] That case, *NAACP v. Alabama ex rel. Patterson*, established a baseline constitutional rule: Violating the anonymity of an organization's supporters is a violation of their First Amendment rights to freedom of speech and association.[60]

As with most constitutional rights, there are narrow circumstances where the Court has agreed that government interests outweigh the freedoms of speech and association protected by the First Amendment. Most notably, in *Buckley v. Valeo*,[61] the Supreme Court upheld the constitutionality of donor disclosure laws for groups engaged in "express advocacy"[62] – the election or defeat of candidates.[63] It found that some state interests were sufficiently compelling to allow for mandatory donor disclosure rules, as long as those rules served "substantial governmental interests" and did not overly burden individual rights, requiring the disclosure requirement to be narrowly tailored to the interest it promotes.[64] This test is commonly known as "exacting scrutiny."[65]

Notable in Buckley and the litany of cases following that carved out the constitutional contours of disclosure laws, the Supreme Court consistently engaged in a First Amendment analysis. That is, the court acknowledged directly the speech and association harms caused by government collection of supporter and donor information and weighed those factors against government interests. While First Amendment concerns are regularly brushed aside in other government surveillance contexts, the Court has often found a way to protect the free speech and associational rights in the context of donor disclosure requirements without crippling important government interests.

Recently, in *Americans for Prosperity v. Bonta*,[66] the Court struck down a California law requiring the disclosure of donors from all charities to the state.[67] In it, the Supreme Court recognized that disclosure laws chill speech and association when the government collects the record, "even if there [is] no disclosure to the general public."[68] It also provides a guide post for how governments need to think about First Amendment rights in the disclosure context. Governments cannot simply demand disclosure because they want it. A generalized governmental interest in disclosure is insufficient grounds, ipso facto, to violate First Amendment rights.

---

[59] *NAACP v. Alabama ex rel. Patterson*, 357 U.S. 449, 462 (1958).
[60] *Id.* at 462–63.
[61] 424 U.S. 1 (1976).
[62] *Id.* at 45–48.
[63] *Id.* at 66–68.
[64] *Id.* at 68.
[65] *Id.* at 93–94.
[66] 549 U.S. __, 141 S.Ct. 2373 (2021) (slip opinion).
[67] *Id.* at 2385–89.
[68] *Id.* at 2388.

The reason donor disclosure laws are regularly examined through a First Amendment lens lies in part because most donor disclosure laws target speech and association related to politics or political issues. Given the heat of political debates in America, it is perhaps unsurprising that these types of government reporting requirements lead to significant harms to the freedom of speech and free association. These harms manifest in three broad categories.

In *Americans for Prosperity Foundation*, donors to the controversial organization founded by lightning rod libertarian philanthropist Charles Koch provided evidence that supporters to the organization "have been subjected to bomb threats, protests, stalking and physical violence."[69] When donors' addresses are published online, accessible with the click of a mouse to anyone with an Internet connection, the cost for contributing to a cause or charity, particularly a controversial one, is greatly heightened.

But the chill on free speech and association expands well beyond direct threats of violence. In today's highly polarized society, economic costs for supporting political causes can also be high. Donor disclosure gives opportunity for your political opponents to organize boycotts or start pressure campaigns to shut down your business or get you fired. A 2020 survey found that 50% of strong liberals supported firing donors to the presidential campaign of Donald Trump.[70] Similarly, 36% of strong conservatives supported firing donors to the Biden campaign.[71] One can debate whether support for the opposition presidential candidate is worth losing your job over, but if we extend that thinking to every controversial topic – support for pro-life and pro-choice organizations, for Black Lives Matter, or the National Rifle Association – there are few popular causes a person could support that would not expose them to the stigma of being viewed adversely by others. Americans should not have to choose between advocacy protected by the First Amendment and the right to earn a living.

The most significant threat from the mass collection of supporter information comes from governments themselves. In the 1950s, southern states sought donor information to the NAACP for unmistakable reasons. With that information, Alabama had and would continue to "expose members to economic reprisal, loss of employment, threats of physical coercion and other manifestations of public hostility."[72] While few abuses of this power rivals its exercise by the southern states in the 1950s, a lesser manifestation of the same threats continues to this day. In 2012, rogue employees at the IRS leaked donor information from the National Organization for Marriage to the Human Rights Campaign—who then gave the confidential records to the press.[73]

---

[69] *Id.*

[70] Emily Ekins, *Poll: 62% of Americans Say They Have Political Views They're Afraid to Share*, Cato Institute. https://www.cato.org/survey-reports/poll-62-americans-say-they-have-political-views-theyre-afraid-share

[71] Id.

[72] *NAACP*, 357 U.S. at 462.

[73] Mackenzie Weinger, *IRS pays $50K in confidentiality suit*, POLITICO (June 6, 2014 8:28 PM EDT), https://www.politico.com/story/2014/06/irs-nom-lawsuit-108266.

In 2021, California published the personal information of state residents who applied for a concealed carry permit.[74]

The bottom line is donor disclosure laws are dragnet surveillance efforts by government agencies with the goal of capturing private information about organizations for policy reasons—reasons that change from one administration to the next. And the information captured will inevitably be weaponized to chill First Amendment activity. Governments have shown they cannot be trusted to protect that private information.[75]

While the Roberts Court, with its majority of conservative, Originalist judges has steered constitutional jurisprudence toward reliance on the historical underpinnings and Founding-Era meanings of the freedoms defended by the Bill of Rights, the development of constitutional law through the courts is a slow process better measured in half-centuries than years. If policymakers favor strong protections for free speech, association, and privacy in the context of donors' information, there is much room to improve on the uncertain protections recognized by the courts, particularly as the steady drumbeat of increasing regulation carries forward from one administration to the next in executive offices from city to city, state to state, and federal agency to federal agency.

RECOMMENDATIONS

A. Legislation should place limits on the power of governments to condition permits, licenses, or benefits on agreeing to warrantless searches.

State-level legislation would likely be effective in setting out a framework under which state and local agencies may not condition licenses, permits, or benefits on warrantless searches without cause. One solution is for states to adopt legislation that prohibits state and local officers and bureaucrats from engaging in warrantless administrative searches of persons, houses, papers, and effects. To allow warrantless regulatory inspection schemes targeted at dangerous activities that impose serious risks of externalities—munitions factories, distilleries, underground mines, or caustic chemical plants, to remain—such legislation could include a proviso for dangerous and closely-regulated activities. This flips the traditional legislative approach of allowing vague administrative search powers with some exceptions for privacy, to protecting privacy first, and then categorically limiting exceptions.

One problem contributing to the proliferation of warrantless "regulatory" search powers is the vague definitions of "inspections" in authorizing legislation, which does not set out in express

---

[74] Gregory Yee, *Leak of California concealed-carry permit data is larger than initially reported*, L.A. TIMES (June 29, 2022 6:42 PM PT) https://www.latimes.com/california/story/2022-06-29/california-concealed-carry-weapons-permit-data-exposed-in-leak.

[75] See Jim Sciutto, *OPM government data breach impacted 21.5 million*, CNN (July 10, 2015 1:15 PM EDT), https://www.cnn.com/2015/07/09/politics/office-of-personnel-management-data-breach-20-million/index.html; Jada F. Smith, *Cyberattack Exposes I.R.S. Tax Returns*, N.Y. TIMES (May 26, 2015), *available at* https://www.nytimes.com/2015/05/27/business/breach-exposes-irs-tax-returns.html; Philip Ewing, Report: Hackers Stole NSA Cybertools in Another Breach Via Another Contractor, NPR (Oct. 5, 2017 3:48PM ET), *available at* https://www.npr.org/2017/10/05/555922305/report-hackers-stole-nsa-cybertools-in-another-breach-via-another-contractor.

terms whether inspections are to be warrantless, consent-based, complaint-based, or the specific punishments, if any, for refusal. Legislation could fix this problem by stating that no warrantless regulatory inspection power is operative unless it is expressly authorized by legislation specifying that *warrantless* searches are authorized. Unless the statute itself (not a mere regulation) states that a search power is to be warrantless, it is presumed to be dependent on the consent of the property owner, business, or licensee. Such a requirement would prevent local and state agencies from interpreting vague authorizations to inspect as granting them the power to engage in *warrantless* inspections without consent or to punish the failure to consent to such inspections.

Another possible policy solution would be to require an express finding by the legislature that an industry poses a severe danger to the public before including warrantless inspections within a statutory framework for regulation of that industry.

A similar legislative revitalization could occur in Congress with the Right to Financial Privacy Act. Congress should eliminate the exceptions to privacy protections that have swallowed the purpose of the law. In such an instance, citizens would at least be aware of and be able to legally challenge financial transaction surveillance.

Congress and state legislators should also adjust thresholds in surveillance legislation, both regarding financial transactions and regarding disclosure, to account for inflation. Many of these laws when enacted had high enough thresholds that only a narrow sliver of citizens were affected, but the passage of time and passive legislatures have meant that more and more transactions and thus more and more Americans are subjected to the liberty harms of these laws. Inflation adjustment has the added advantage of making it easier on law enforcement by limiting the world of monitored transactions to only those most likely to be indicative of wrongdoing.

Finally, pushes for any type of privacy legislation should not neglect the First Amendment harms of the current government surveillance regime. Privacy is a difficult value to argue for – it is subject to Boiling Frog Syndrome. While privacy is important in the aggregate, invasions of privacy slowly encroach in unassuming and often convenient ways. Not so with free speech and association violations; when stories of First amendment violations come to light – whether the retaliatory search of a reporter's home or the shutting down of a church service – it elicits strong reactions that can be used to advance these necessary privacy protections.

The rationale for stronger restrictions on government search powers are compelling. First, warrantless searches as a condition for licenses, permits, or benefits can lead to potential abuses of power. Without proper legal safeguards, government agencies could overreach and conduct searches that are not justified by any specific suspicion of wrongdoing. This not only erodes trust in government but also creates a slippery slope where the boundaries of individual privacy become increasingly blurred. Legislation can help define the scope and limitations of such searches, ensuring that they are conducted only when necessary and in a manner that respects individuals' constitutional rights.

Second, imposing warrantless searches as a condition of obtaining licenses or benefits may deter individuals from exercising their rights or seeking assistance from the government when needed.

People may be hesitant to apply for government programs or permits if they fear that their privacy will be compromised. This can have detrimental effects on public health, safety, and welfare, as individuals may avoid seeking necessary services or permits due to concerns about unwarranted intrusion into their personal lives. Legislation can provide clarity on when and how these searches can be conducted, giving individuals greater confidence to engage with government agencies without sacrificing their constitutional rights. In summary, legislation restricting the power of government to impose warrantless searches as a condition of licenses, permits, or benefits is crucial to preserving individual rights, safeguarding against potential abuses, and maintaining public trust in government institutions. It ensures that searches are conducted only when justified, and that the balance between security and privacy is maintained.

B. Warrant requirements and minimization procedures will better safeguard privacy in the face of dragnet surveillance or geofence collection than the status quo.

Currently, courts are left to meander their way through questions regarding whether a warrant is required for the collection of geofence data, networked traffic camera footage, or facial-recognition information assembled from vast datasets. While they will likely reach a consensus that specific warrants and minimization procedures should be required in these cases—this has been the trend of Fourth Amendment jurisprudence lately—there is a great deal of harm in the interim from misuse of these surveillance tools. With respect to searches and seizures, the courts' role is one of screening, ensuring that the government has satisfied the Fourth Amendment's requirements of probable cause (a sufficient likelihood of finding evidence) and particularity (the warrant limits the discretion of officers engaged in a search or seizure).[76] But this is not the first time courts have encountered difficult questions posed by advancements in technology that make the collection of third parties' private conversations or information likely, even when executed under the authority of a warrant.

Historically, when courts have been confronted by a proposed search that could sweep broadly to include sensitive information from persons who are not the targets of an investigation, they have insisted on "minimization procedures" – essentially rules officers follow when executing a warrant that minimize their interference with citizen's privacy interests. This issue came to the public's attention recently when a police department executed a "sneak-and-peek" warrant at a massage business in Florida with the intention of catching particular patrons seeking prostitution services, but the warrant did not limit the officers monitoring surveillance equipment from watching patrons not under investigation from undressing.[77]

Because sneak-and-peek warrants are broader in time and scope than a conventional warrant, courts have required that the applications for these warrants include suggestions for limiting the monitoring of the surveillance devices and collection and retention of their data so as to minimize their interference with the privacy interests of persons not under investigation. For example, it could include requiring a police officer to turn off the recording of a wiretap after identifying that the phone call is between a lawyer and their client, or does not include a person who is being

---

[76] See U.S. Const. amend. IV.

[77] Terry Spencer, *Judge: Kraft's prosecutors cannot use massage parlor video*, ASSOCIATED PRESS (May 13, 2019 6:11 PM CDT).

investigated under the warrant. Similar restrictions could provide backstops against the use of dragnet surveillance.

The imposition of minimization procedures on warrants for geofence data or dragnet surveillance is of great importance in safeguarding against potential abuses and intrusions while also upholding the privacy rights of third parties who are not the primary targets of investigations. Such legislative features would make enforcement agencies more accountable and help mitigate the indiscriminate collection of data that disproportionately infringes upon innocent individuals' privacy. By requiring minimization procedures, legislation could strike a delicate balance between the government's investigative powers and the preservation of civil liberties.

C. Policy solutions should be targeted at restraining government power, not limiting end-users, market innovation, or freedom of contract.

In the digital age, the protection of fundamental freedoms such as privacy, speech, and association is of paramount importance. But solutions cannot and should not stifle the technological innovation that created the digital age in the first place. Rather than imposing restrictions on private end-users and corporations that could make technology worse and curtail freedom of contract, the focus should be on limiting the government's unchecked power to collect, maintain, and exploit private data.

First and foremost, limiting government data collection is essential to preventing dragnet surveillance. When the government has unrestricted access to vast amounts of private data, it creates the potential for abuse and overreach, eroding the very foundations of privacy. Legislative measures should emphasize transparency, oversight, and strict limitations on the data that government agencies can access. This includes what data the government is permitted to buy from third parties. By holding the government accountable for its data collection practices, we can better protect citizens' rights without hindering the private sector's ability to innovate and provide valuable services.

Imposing broad restrictions on private end-users and corporations regarding data collection and usage can have detrimental effects on innovation. Many technological advancements and services rely on the responsible collection and analysis of data, whether for improving products, enhancing user experiences, or addressing societal challenges. This has been for the better. It allows your phone to know what kind of restaurants you might like, where your dog has run away to and whether an alarm has gone off in your home. Excessive regulation in this regard may stifle creativity and hinder industries that rely on data-driven insights, ultimately impeding progress and economic growth. Modern threats to privacy and association require modern solutions that work with, not against, the technology we have.

Limiting how private entities collect and use data could encroach on freedom of contract. Individuals should have the autonomy to engage in voluntary agreements with service providers and businesses, and this includes consenting to how their data is handled in exchange for services. Heavy-handed restrictions on data practices could disrupt these contractual relationships, curtailing the freedom of individuals to make informed choices about the products and services they use. And ironically, limiting individuals' freedom of association.

Thus, legislative solutions should prioritize restraining the government's power to purchase or collect data downstream rather than imposing burdens on private commercial transactions. Such an approach will bridge the current gap in the case law that makes it difficult to sue the government under the Fourth and First Amendments to prohibit its collection of private user data when it has either purchased it from a third party or collected it through recordkeeping requirements imposed on heavily regulated industries, such as the financial sector.

The federal and state governments are entities of limited and enumerated powers. Their agencies, departments, and bureaucrats by extension are likewise limited by the statutes that define their scope. Laws that place limits on the power of these agencies to obtain and retain private user information would serve as a useful check on expansive surveillance.

And when government is permitted to collect or access private informational datasets, limiting the permitted duration that it can be kept helps mitigate the chilling effect on free speech and association. By setting reasonable time constraints on data retention, we minimize the risks associated with data breaches and unauthorized exposure. This approach also ensures that irrelevant information is expunged, reducing the potential for abuse and political targeting.

Finally, stringent security requirements, including encryption and access controls, bolster trust and confidence in data protection, reassuring individuals that their information is safeguarded. While by no means sufficient in and of themselves, taking data security seriously demonstrates at least a nominal commitment by the government to privacy interests. Over time, successfully safeguarding this data can lead to greater public confidence that there won't be government leaks. It may even permit a more balanced approach that respects both national security concerns and individual freedoms.

D. Proposed legislation should include a private right of action in the courts to enforce limits on government surveillance.

Ensuring the effectiveness of legislative restrictions on the use of surveillance technology is critical. Proposed legislation must, therefore, possess the means to hold violators accountable. Providing individuals affected by violations of such legislation with the right to seek relief in the courts is an important safeguard against the intrusions to civil liberties contemplated by increasingly sophisticated government surveillance.

Creating a cause of action for individuals to seek relief in the courts serves as a powerful deterrent against potential abuses of surveillance technology and should thus be a feature of any legislative attempt to rein in the arbitrary use of broad government surveillance. When those state actors who deploy such technologies know that their conduct is reviewable in the courts, they are incentivized to adhere to the limits and safeguards established by legislation. This not only fosters a culture of accountability, but also encourages responsible and ethical use of surveillance tools.

Providing individuals with the opportunity to seek relief in the courts also empowers them to protect their rights and seek justice when those rights are violated, aligning societal incentives with oversight and accountability. If the government has violated your civil rights, you deserve your

day in court. Otherwise, legislative restrictions on government surveillance will be mere political posturing.

To strengthen legislative restrictions on surveillance technology and protect individual liberties, the right to seek relief in the courts should be a fundamental component of any proposed legislation.

E. Targeted impact litigation to enforce First and Fourth Amendment rights in the face of increasing government surveillance should not be neglected as a vector for effecting change.

Recent Supreme Court precedents have introduced a new paradigm, offering a crucial opportunity for impactful litigation centered around the First and Fourth Amendments. Rulings like *AFP v. Bonta*, *Carpenter v. United States*, *City of Los Angeles v. Patel*, and *United States v. Jones*, discussed above, have created new opportunities for litigation to limit the intrusion of government surveillance on civil liberties.

When the Supreme Court said in *AFPF v. Bonta* that "the disclosure regime burdened the associational rights of donors" it was certainly true. But as we have seen, that burden is not unique to donors. Licensure requirements and their accompanying administrative searches burden the association rights of businesses, hobbyists, and homemakers. Financial transaction surveillance burdens the association rights of anyone with a bank account. Geofencing and mass electronic surveillance burden the association rights of nearly everyone.

It is little more than an accident of history that the rules, standards and precedents for donor disclosure laws have been litigated almost exclusively through a First Amendment lens and not a Fourth Amendment, "due process," or generic privacy lens. But the Supreme Court, not unlike the public, has been more protective of First Amendment interests than of generic privacy interests. To that end, it would be wise for litigants challenging these laws to do so explicitly on First Amendment grounds.

This is not to say that crying "First Amendment!" is some sort of legal trump card. Far from it. The government likely will convince courts of their compelling need and for many surveillance regimes. But raising First Amendment arguments forces courts to grapple with doctrinal questions that take very seriously the rights of citizens. In particular, First Amendment standing doctrine provides broader opportunities to have one's day in court than is the case under many other types of legal claims.

Similar opportunities to use the Fourth Amendment as a wedge against intrusive surveillance have also emerged. The Court's recognition that a cause of action can accrue from a government trespass to property, notwithstanding societal expectations of privacy, gives litigants an opportunity to challenge many of the court precedents that guard government surveillance powers. For example, the third-party doctrine, discussed above, is a product of the era in Supreme Court history when the Court *only* looked to societal expectations of privacy. In *Carpenter*, the Court took a bite out of the third-party doctrine by holding that cell phone users have a reasonable expectation of privacy in their location data even though it is shared with their telecommunications providers through cell

towers. If the litigants challenging the search in *Carpenter* had brought their cause of action under the trespassory cause of action recognized by the Court in *Jones* rather than the invasion-of-privacy theory, they might have avoided the hurdle imposed by the third-party doctrine altogether. Justice Gorsuch, writing for the dissent in that case, seemed to encourage future litigants to try this approach.[78]

Likewise, a great many of the state and federal court precedents upholding warrantless searches of businesses were the products of the Supreme Court's privacy era. Targeted lawsuits challenging regulatory searches as trespasses to property rather than invasions of privacy may yield precedents more favorable to the security of property and the right to demand a warrant. Unlike invasion-of-privacy cases, trespass-to-property lawsuits under the Fourth Amendment are evaluated based on common-law property principles and the historical restrictions on particular customs, businesses, practices, and uses of property. They do not rise and fall with the vicissitudes of societal expectations of privacy.

While relief through the courts may be slow, precedents set in constitutional cases have more staying power than legislation because of the legal doctrine of *stare decisis*. Thus, while legislation might provide some relief, impact litigation should not be neglected as an effective measure for accomplishing lasting and powerful restrictions on intrusive government surveillance.

[78] *Carpenter*, 138 S.Ct at 2264.