

Statement before the Pennsylvania House Republican Policy Committee
On Protecting the Fourth Amendment: Establishing Guardrails for Automated
Surveillance

Flock Camera Systems and Mass Surveillance in Fourth Amendment Perspective

JIM HARPER

Senior Nonresident Fellow

September 27, 2026

EXECUTIVE SUMMARY

We have seen enormous progress in information technology thanks to the twinned advances of miniaturization and digitization. We have surrounded ourselves with digital sensors that easily capture and store information, making it available for transfer and processing. The benefits are tremendous, but these advances also come with costs.

Privacy costs are one. Our communications, health information, financial information, and movements are all captured and digitized. Directly or through inference, that puts troves of detail about our private lives at risk. And it threatens liberty when such private information is in the hands of the most powerful institutions.

Today Americans' instinct for maintaining the American experiment has been given voice through the debate about Flock cameras. With public opinion urging us on, I offer the Fourth Amendment as a framework for thinking about this problem.

We can recognize digital seizures and digital searches, placing them under the same constitutional control as their analog counterparts. Flock cameras are arguably a seizure of Americans' information. More clearly they are a search of and for Americans' cars, conducted all of the time. By close inference, they are a search for all drivers, all of the time.

That leaves the question of whether operating Flock and similar camera systems is reasonable. The Fourth Amendment offers several guideposts suggesting they are not, but the privacy-security tradeoff invited by the Fourth Amendment is always up for revision.

In response to Flock camera systems, there has been litigation, which will inform the debate. You are hearing from a leader on legislation to control these systems in New Hampshire. There are numerous ways that Flock and similar systems can be given guardrails, which may make them reasonable in both constitutional and ordinary terms.

While you address the Flock issue directly, I recommend that you also work to control the parallel data streams that can be just as revealing as mass surveillance through Flock cameras. New Hampshire again may offer a model in the Common Law Privacy and Consumer Protection Act, which would recognize ownership of private data, and thus constitutional protection for it, even when stored with third parties such as cloud service providers.

Chairman Rowe and members of the committee—

Thank you for the opportunity to testify remotely before your committee. The wonders of technology include the ability to join you from New Hampshire today. Along with the enormous good it does, advanced technology comes with costs, including threats to privacy and liberty. Those we must work to control.

I am Jim Harper, a nonresident senior fellow with the American Enterprise Institute and a senior research fellow at the University of Florida's (UF) Levin College of Law. For more than twenty-five years, I have been a policy analyst specializing in the intersections among law, technology, and society. My legal education focused on constitutional law, and my major area of professional focus has been privacy. With UF Professor Jane Bambauer, I am the co-author of the forthcoming legal casebook, *PRIVACY AND PERSONAL INFORMATION LAW*.

I am amused and startled to say that I predicted this problem a whopping 25 years ago. Asked to testify about red-light cameras to the U.S. House Transportation and Infrastructure Committee in July, 2001, I said,

Red light cameras are only the first installation of the Big Brother infrastructure. There's very much more to come, and very soon, too. Optical character recognition, for example, may already allow red light cameras to read license plates and scan for specific cars. Networked cameras will be able to track cars as they travel through a city and on the highways. Database technology will make it possible to record the movements of cars and make a permanent record of them if they've been captured on camera.¹

I suppose I was wrong to say it was happening soon, and I thought it might be red-light cameras. I did not predict the creation of a business sector to provide surveillance as a service to government entities, but I did pretty well with this prediction.² I guess young people aren't always wrong.

The challenge we are looking at arises from two related technology trends: miniaturization and digitization. I'll address each briefly, then turn to their consequences and what we can do.

¹ Statement of Jim Harper, Editor of Privacilla.org, to the U.S. House of Representatives, Committee on Transportation and Infrastructure, Subcommittee on Highways and Transportation an "Automated Enforcement—Red Light Cameras" (July 31, 2001), https://commdocs.house.gov/committees/trans/hpw107-40.000/hpw107-40_of.htm.

² Ten years ago, I identified the license plate as an important root of this problem. Jim Harper, "The End of the License Plate," *Washington Examiner* (Apr. 18, 2015) <https://www.washingtonexaminer.com/opinion/2051674/the-end-of-the-license-plate/>. More on that curious idea below.

Miniaturization and Digitization

Thanks to enormous advances in materials science, manufacturing, and other technologies and sciences, countless machines and devices that used to be bulky and costly to operate are today small, lightweight, and energy-efficient.

You only have to think of the camera to illustrate how miniaturization has worked. The camera came into existence in the early 1800s. By 1890, early portable cameras weighed between one and five pounds. Film had to be carried separately, of course, and photographers had to load and unload it as they captured images on a light-sensitive chemical medium.

Today, cameras weigh—well, close enough to nothing. They are so lightweight and small that we think nothing of having two of them built into the typical cell phone, one each on the front and back. There is no film to carry. And we can choose seamlessly between still photography and video and sound recording.

Cameras capture imagery and sound by converting those signals to digital content, which is stored right there on the phone so efficiently that we can produce hours of recordings before needing to offload them from our phones to some other lightweight, low-cost storage device.

They can do so because of digitization. Simply stated, digitization is the practice of converting information to metaphorical “ones” and “zeroes.” There are a wide variety of protocols and media that record those “ones” and “zeroes” in different ways with astounding efficiency. Having information in digital form makes it not only easier to capture and store, but also easier to transfer and process.³

Miniaturization and digitization have multiplied data collection hundreds of times over the status quo of a few decades ago. Think of this in terms of “sensors,” devices that capture information and prepare it for storage, transfer, and use. There are many more sensors than the camera.

We are Awash in Digital Sensors

Cameras are but one of countless “sensors” that have proliferated across the human landscape. The word “sensing” refers to any gathering of information, including capture of analog light and sound waves by the eyes and ears. I use the term here to refer to the gathering of information about the world as digital data.

Sensing of information, including personal information, has exploded as we have surrounded ourselves with sensors that digitize information about ourselves and our surroundings. People buy device after device, each doing its work by converting analog information to digital.

³ This discussion is drawn from and much expended upon in Jim Harper, “Privacy and the Four Categories of Information Technology,” American Enterprise Institute, May 26, 2020, <https://www.aei.org/research-products/report/privacy-and-the-four-categories-of-information-technology/>.

Like cameras do with visual and auditory information, keyboards in every modern phone translate people's correspondences and writings into digital form. Every email, text message, and writing we send is analog information converted to digital data. Other sensors on many phones include accelerometers, gyroscopes, magnetometers, and barometers. Our phones interact with the Global Positioning System to sense and record our location information. Our cars are packed with sensors. Our homes have sensors throughout, gathering temperature, motion, sound, and occupancy, to name a few. The list of sensors and sensing systems goes on and on.

All of these things bring us stupendously great conveniences, entertainments, comfort, and safety. But those benefits come with costs and risks.

Consequences

Think now of all the data and data types in the vast enterprise we have built—our communications (including phone conversations, emails, texts, and online chats), health information (including medical records, diagnoses, lab test results, prescriptions, body scans, health insurance, and billing details), financial information (purchases, loans, payments, assets, investments), and movements (air travel, auto travel, and just walking around) are all captured and digitized.

The information in each category is useful, but it is even more useful when combined and recombined. New vistas and opportunities are opening all the time, as technologies continue to emerge and combinations of data are found that will expand our horizons in every direction. We are getting underway now with “artificial intelligence.” The leading variant, the large language model, approximates reading and other perception such as looking at pictures to deliver content that approximates thought and creativity. The benefits will be huge. I don't think the costs include the end of humanity, but there will be costs.

Significant costs come with many advances, and in the information technology field privacy is one of them. The wonderful practical daily uses that we can make of all this data have something of a sinister side. Communications data, health data, financial data, location data, and the rest can directly or in combination tell others about our family lives and intimacies; our medical and mental health diagnoses and treatments; our foibles, failures, and betrayals; our religious beliefs and practice; political leanings and activities. The list goes on and on.

Many or most of these things people prefer to keep private. People must have privacy to feel free, to feel the sense of authority over our own lives that we expect as Americans. When our information is exposed to powerful actors, those privacy costs are also liberty costs. The aphorism “information is power” tells the story in an accessible way. People are right to be concerned that large organizations may come to know too much about them. Lost privacy makes us susceptible to manipulation and control. Having privacy insulates us from a future—however unlikely it may seem now—of totalitarian control that we see in China under its “social credit” system of digital mass surveillance.

The tradition of freedom and the exceptional nation our American forefathers built is a form of human progress that is not naturally self-perpetuating. We are obligated to design our future so that American liberty will survive.

Mass Surveillance

Today, that instinct for the survival of the American experiment has been given voice through the debate about Flock cameras. The public is very concerned that tools of mass surveillance are being turned on them without justification. (Flock is a brand, of course, which made itself conspicuous by adopting a name that suggests we're sheep. The subject matter is mass tracking and warehousing of information about the location of Americans' cars, which implies the locations of drivers.)

If I may venture to interpret public opinion, Americans perceive these systems as reversing the presumption that people are innocent until proven guilty. Flock cameras subject all of us to watching in case we do something wrong, and that is not how the American system works. Americans reject a system that could be used to shift power from its true source, the people, to government actors and agencies that are supposed to work for them, not on them.

These debates can be unfair. The public may rely on cherry-picked evidence and demagoguery. But we can gather valuable signals about real issues all the same: the public's intuition is that mass surveillance is out of step with their values.

Fourth Amendment Principles

A rock-solid expression of American values in terms of privacy and security is the Fourth Amendment. The Fourth Amendment is not just the law of the land; it is also an eminently sensible way of organizing our thinking about government access to information about people. It protects privacy, yes, and it also helps direct law enforcement investigations toward logical inferences about real suspects, away from fishing expeditions and other wasted effort.

The Fourth Amendment says, in relevant part:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated.

Unreasonable searches and seizures are out. Reasonable searches and seizures are in.

Now let's align these Fourth Amendment concepts with the digital world. The good news is that the concepts of "search" and "seizure" can be applied to digital stuff.

Digital Seizure

I will start with seizure because seizures are very often the opening part of a search. This is true online

and off. In the classic 1968 case that recognized the pat-down as a reasonable seizure and search, *Terry v. Ohio*, law enforcement officers stopped a suspicious person (the seizure) and patted him down for weapons (the search).⁴

The seizure concept has a deep legal pedigree in property law. Other seizures that the Supreme Court has recognized (more or less clearly) include moving stereo equipment, helping take a mobile home from its owner, entering someone's property to bring a drug-sniffing dog to their front door, and attaching a GPS device to a car. We all recognize these items of personal property and real property. It is less common to hear now, but John Locke wrote in his *Second Treatise of Government*, "every man has a property in his own person." We own our bodies.

The Supreme Court has not yet clearly found that digital materials we store privately are our property. It has suggested as much in a case dealing with the search of cell phones. Justice Gorsuch has argued cogently that the Court should use property rights to administer the Fourth Amendment with respect to our private data.

But right now personal and private information that we create using our digital devices is not clearly recognized as our property. Under the Supreme Court's misbegotten "third-party doctrine," anything shared with a third party is not constitutionally protected. Every last bit of our communications pass through service providers—ISPs, email service providers, cell phone providers, and so on—so none of it is clearly protected.

We are at risk of mass surveillance through these service providers. Think again of all the data: communications, health information, financial information, location information, things that reveal intimate and highly personal matter. When such data is housed with service providers and government agents come calling, they do not need to meet the Fourth Amendment's probable cause standard for seizing our data. The moment your information leaves your phone or computer, weak and inconsistent statutory standards take over.

There is a good argument that the operation of Flock cameras for government entities involves a seizure of property, too. Amy Peikoff of the Pacific Legal Foundation argues that the mandatory license plate, which one must display to drive legally on the roads, created an easement on our cars that allowed for occasional observation and identification. Using that small seizure of our cars for administering traffic safety seems quite reasonable. But using it for developing an archive of drivers' movements without any suspicion of wrongdoing abuses the easement.⁵ That is a trespassory search of the car, which is a Fourth Amendment "effect."

More familiar will be the idea that Flock cameras represent a constant ongoing search for the whereabouts of all cars and their owners.

⁴ *Terry v. Ohio*, 392 U.S. 1 (1968)

⁵ Amy L. Peikoff, *The Record, Not the Lens: ALPR Retention, Property, and the Fourth Amendment*, 28 N. Car. J. L. & Tech, (forthcoming April 2027), <https://ssrn.com/abstract=7280339>.

Digital Search

The “search” concept doesn’t have the same legal contours that property law gives to seizure, but we can recognize digital searching. Thus we can decide when it is, and when it is not, reasonable.

A Supreme Court case that I think is very instructive is *Kyllo v. United States*⁶ from 2001. It is helpful because it was a high-tech search case without any seizure. In *Kyllo*, government agents stood on the public sidewalk and aimed a thermal imager at a private home without a warrant. Excessive heat on one side of the home helped confirm their suspicions about what was going on inside, and they convinced a judge to give them a warrant. That ultimately revealed a marijuana grow operation.

Justice Scalia wrote for the Court that the use of the imager on the home was a search of it, which required a warrant. “Where, as here, the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a ‘search’ and is presumptively unreasonable without a warrant.”⁷

Consistent with his focus on originalism and textualism, Justice Scalia used a dictionary definition of search in *Kyllo* to flesh out his thinking. “When the Fourth Amendment was adopted, as now, to ‘search’ meant ‘[t]o look over or through for the purpose of finding something; to explore; to examine by inspection; as, to *search* the house for a book; to *search* the wood for a thief.’ N. Webster, *An American Dictionary of the English Language* 66 (1828) (reprint 6th ed. 1989).”⁸ The Court has used that definition a number of times since.

We can recognize “searching” through directed effort to find something. In a 2017 article for the National Constitution Center, I delved further into the search concept, particularly in the high-tech world, which works a little differently. In “Administering the Fourth Amendment in the Digital Age,”⁹ I wrote about how search worked in the context of facial recognition:

Searching has two conceptual parts, which generally occur in a particular order. First, the specific thing to be searched for is identified. Next, the field in which it may be found is examined. Searching a forest, for instance, involves identifying the person, instrumentality, or evidence to be found, then marching through the area with eyes peeled for that thing. Facial recognition reverses these processes. It collects the material to be canvassed—facial signatures—then at any later time canvasses the earlier-collected facial signature data for a match. The fact that the steps in the process are reversed should not change the conclusion that

⁶ 533 U.S. 27 (2001).

⁷ *Id.* at 40.

⁸ *Id.* at 32.

⁹ See Jim Harper, *Administering the Fourth Amendment in the Digital Age*, National Constitution Center: A Twenty-First Century Framework for Digital Privacy white paper series (May 2017) <https://constitutioncenter.org/media/files/harperfinal5.pdf>.

facial recognition is a search technology and the use of it is a search. Conversion of a facial image to a facial signature that can be scanned for matches is a search of the face itself to render data that make the face amenable to being the object of a later search. It is enough of a step in the process of searching that it is best recognized as a search occurring at the time the processing is done.

It is easy to recognize the similarity between facial recognition and Flock cameras. Flock and similar systems collect all the material to be canvassed, license plates and other unique characteristics of automobiles. At any later time, government agents can use the earlier-collected automobile signature data to find a match. Flock cameras are for searching, it seems to me, and what they do is searching.

Generally speaking, one does not seize information by gathering what is publicly displayed. (Amy Peikoff's argument, noted above, creates interesting questions about information that government has mandated to be displayed.) I do believe that processing publicly available information at a certain level of intensity is "searching." In my opinion, the processing of imagery to identify license plate numbers and to create "signatures" from other distinct characteristics of cars is searching those cars. There is no other reason to subject imagery to such processing than the (later-to-be-used) "purpose of finding something."

Flock cameras are reminiscent of a monitoring system put in place over Baltimore a decade ago. In 2016, Baltimoreans learned that their police department had hired a company called Persistent Surveillance Systems to circle the city taking high-resolution photographs for hours on end each day, weather permitting. The collected imagery could be searched later to examine who had gone where.

Suspended by the city once it was publicized, the system also was challenged in court. The U.S. Court of Appeals for the Fourth Circuit found that it violated Baltimoreans' reasonable expectations of privacy to have a system in place that could so readily and comprehensively determine their locations and movements.¹⁰

The "reasonable expectation of privacy" test is the dominant Fourth Amendment rule—a search will be found when government activity violates privacy expectations. The weakness of that doctrine is such that I recommend using more concretely legal frameworks. Consistent with the trend toward textualism in the Supreme Court, I have been writing here about the meaning of the words "search" and "seizure," as you've seen.

It is in-bounds, of course, to find that Flock cameras violate Americans' reasonable expectations of privacy. I believe people do not expect to have their whereabouts tracked as they go about their ordinary business on the streets of their neighborhoods and cities. The converse is that they expect not to be tracked. It violates their privacy when they are tracked.

Flock cameras are an ongoing digital search of and for all cars and by inference for their drivers. The

¹⁰ *Leaders of a Beautiful Struggle v. BPD*, 2 F. 4th 330 (4th Cir. 2021).

practice of mass surveillance of this type is a somewhat predictable result of miniaturization and digitization, along with our demand for safe streets. That does not dispose of the issues. The next question is whether maintaining Flock camera systems to search for all cars and drivers is reasonable.

Are Flock Camera Systems Reasonable?

The “fulcrum” of the Fourth Amendment, properly interpreted, is the question whether a given search or seizure is reasonable.¹¹ This the most subjective, value-laden part of the question, but the Fourth Amendment has some clues and guideposts.

First, understand that the word “reasonable” at the time of the Framing was not meant to ask about feelings. The implication of the word “reasonable” is that a search or seizure, to be valid, must be supported by reason. A given search or seizure must lead relatively directly to evidence or fruits of crime. It should not be a speculative stab at something that only possibly could turn up useful information.

The Fourth Amendment suggests strongly that a seizure or search is reasonable when it has been approved by a neutral magistrate. Law enforcement agents must articulate to someone not involved in an investigation how the action they are planning to take is likely to support the investigation.

There are exceptions to the warrant requirement, of course, such as when some exigency such as a killer on the loose or a recent kidnapping make it unwise to take the time to get a warrant. But most reasonable searches will be articulated and approved ahead of time through the warrant process. Flock camera systems do not have that quality. (Flock data is used in seeking warrants, of course, a reminder of the *Kyllo* case where the result of thermal imaging supported a warrant, but the warrantless imaging violated the Constitution.)

The Fourth Amendment also requires warrants to be narrowly circumscribed (“particularly describing the place to be searched, and the persons or things to be seized”). If the evidence is that a car in a given garage was used in a hit-and-run and will have revealing paint marks on it, the warrant may not permit a search of the bedroom and den, or the house’s computers. Particularity is a tough one for Flock camera systems, as they are searching all cars (or seizing the information) that come before them. The particularity requirement suggests that operating Flock camera systems is not reasonable.

All that does not entirely close out the question. There are certainly law enforcement benefits from collecting and processing all this data. If there were a far greater crime problem in a certain area, maybe it would be reasonable to search the comings and goings of all. Good, clear evidence of stable crime reduction benefits would be an important input into the question whether the public and the law would accept mass surveillance as reasonable. I don’t think it is likely, and the existence of the current debate suggests that the public sees Flock cameras as unreasonable.

¹¹ The “reasonable expectation of privacy” test mashes things up by asking whether expectations of privacy are reasonable and finding an unconstitutional search when reasonable expectations are offended.

But there may be quite a bit more tailored uses of Flock cameras that are reasonable. They might record simple imagery without processing it and then process select imagery gathered in a certain area at a certain time, for example. That would reduce the law enforcement benefit some, while reducing the privacy consequences a lot. These are hard trade-offs.

Given my tentative conclusion that processing is a search, I am less inclined toward another idea for mitigating privacy consequences. That is to process imagery but only allow access to it with a warrant, say, when a particular suspect vehicle is sought.

These types of searches would have many similarities to the “geofence warrant” that was the subject of the *Chatrie* case, which was argued and decided in the Supreme Court earlier this year.¹² The government in *Chatrie* required Google to turn over limited data about all users near a bank robbery, then winnowed down the identifiable information it sought to three people, one of whom was the bank robber. The *Chatrie* Court found that this process was a search (using “reasonable expectations” doctrine). It sent the case back down to the U.S. Court of Appeals for the Fourth Circuit to determine whether the search of all Google users’ data was reasonable. Stay tuned for more.

Responses: Litigation, Legislation, Constitution

What is to be done? First I will note one of the lawsuits happening in this area. More relevant here: You as state legislators have a practical role in designing state policies that bring mass surveillance to heel, and you also have a leadership role in helping establish constitutional thinking and principles in your state and beyond.

In Kansas, a conservative public interest law firm called the Kansas Justice Institute has filed a lawsuit against the city of Wichita arguing that the use of ALPR systems violates the provision of the Kansas Constitution’s that is similar to the Fourth Amendment.¹³ It’s an opportunity to explore how changes wrought by technology can be reconciled with basic concepts and first principles.¹⁴

As legislators, you have a direct role in deciding for the state of Pennsylvania what is “reasonable” in ordinary terms, and that will help influence the constitutional debate. I am aware that you are taking testimony from Neal Kurk, a former representative from New Hampshire, who was a leader on this issue and is a privacy hero in my estimation.

I will defer to his expertise and experience, but I am happy to offer my assistance beyond this testimony,

¹² *Chatrie v. United States*, 146 S. Ct. 2193 (2026).

¹³ See Kansas Justice Institute, “Wichita Automated License Plate Readers” web page, <https://kansasjusticeinstitute.org/case/automated-license-plate-readers/>.

¹⁴ See Jim Harper, “Flock Camera Systems May Face a Constitutional Reckoning,” AEIdeas (Aug. 11, 2026) <https://www.aei.org/domestic-policy/technology-and-innovation/flock-camera-systems-may-face-a-constitutional-reckoning/>.

if it would be helpful in crafting something like what New Hampshire did. As I alluded to above, there may be ways to regulate the installation and use of Flock camera systems that make them reasonable, by putting guardrails around their locations, their collection of imagery, their processing of data, the amount of data they retain, how long they retain data, and how to regulate government agents' access to data, for example. The latter control would curtail misuses that have been widely reported.

In Flock systems, you have a mass surveillance technology that I think is a "search" in constitutional terms. It is also an arguable seizure system, because it relies so heavily on the mandated display of a license plate. You should not control this one source of privacy concern without considering the rest of the challenge.

I emphasized data seizure above because Flock systems are not the only source of data about people's movements. Our cell phones and often our cars themselves produce and help warehouse data that is equivalent to what Flock camera systems do. It would be a small victory indeed, if you brought Flock camera systems under control only to leave in place the parallel mass surveillance that can occur through these other data streams.

Until the Supreme Court figures out the right path on questions about seizure of digital data, leadership on this issue must come from elsewhere, such as state legislatures.

In New Hampshire, legislation has been introduced to recognize and embrace ownership of our private data. The Common Law Privacy and Consumer Protection Act,¹⁵ introduced last year and slated for reintroduction in November for the 2027 term, would recognize that handing private data to a service provider does not extinguish our property rights in such data. Transferring personal information to third parties is presumed to be for safekeeping, just like one might hand their car keys to a valet or put their dog in a kennel.

Storing emails with Google or text messages with Verizon do not make your emails and texts these companies' property. These are transfers of possession, not ownership.

The Common Law Privacy and Consumer Protection Act matches American's intuitions that their information is literally *theirs*. It would mean that accessing Americans' private information requires a probable cause warrant, whether the information is in their homes, on their phones, or stored for them in the cloud. An advocacy organization called the Ludlow Institute has put together a campaign website for the law that tells the story right in the URL: [MyInformationisMyProperty.com](https://myinformationismyproperty.com).

There is plenty of evidence that Americans believe their private data is their own, and there is legal treatment of private data as property, but the courts have been conservative about recognizing private, unpublished data as property, even when service providers store it for us under strict promises of privacy and security.¹⁶ If states adopt the presumption that stored data remains the property of the

¹⁵ H.B. 1436 (NH) https://gc.nh.gov/bill_status/billinfo.aspx?id=1667.

¹⁶ See Jim Harper, Personal Information is Property, 73 Kan. L. Rev. 113 (2024) <https://ssrn.com/abstract=4691923>.

person placing it in safekeeping—the legal term is “bailment”—that thinking would imbue itself into court cases.¹⁷ States cannot amend federal constitutional law, but they can give it a good strong nudge through state property law.

Through the lens of the Fourth Amendment, I have tried today to offer a framework for thinking about the privacy and liberty threats that come from the burgeoning technologies that surround us. The debate about Flock camera systems is one prominent instance of threats that can come from new technology, even as the bulk of the outcomes that come from new technology generally (including safety and security) is on the benefit side of the ledger. I am confident that consumer benefits that will continue to grow—including from “AI.”

The combination of miniaturization and digitization has allowed our vibrant tech industry to create amazing technologies. Along with the clearly good, we get the controversial, such as Flock camera systems. Our job is to mitigate the costs and re-strike the age-old trade-off between liberty and security.

I noted earlier that cameras weighed about one to five pounds in 1890 to illustrate the great change in technology from then to now. But another thing about 1890 is notable. That is the year that Samuel Warren and Louis Brandeis published their seminal Harvard Law Review article, “The Right to Privacy.”¹⁸ They opened by saying that the privacy interest might fall within individuals’ “full protection in person and in property.”¹⁹

The inspiration for their article was a certain type of new technology that they felt threatened privacy: flash photography. The next step in the history of privacy is yours.

¹⁷ The Colorado Supreme Court has ruled that one’s Google search history is the subject of a reasonable expectation of privacy under the Colorado Constitution, and also that a seizure of data about one’s searches from Google violates a property right under Colorado and federal constitutional law. 536 P.3d 1260, 1273–74 (Colo. 2023).

¹⁸ Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

¹⁹ *Id.*