Scientific Research Publishing

Journal of Information Security, 2024, 15, 589-611
https://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

Ending Privacy's Gremlin: Stopping the Data-Broker Loophole to the Fourth Amendment's Search Warrant Requirement

Samantha B. Larkin, Shakour Abuzneid

Department of Cybersecurity, Roger Williams University, Bristol, USA
Email: slarkin749@g.rwu.edu, sabuzneid@rwu.edu

How to cite this paper: Larkin, S.B. and Abuzneid, S. (2024) Ending Privacy's Gremlin: Stopping the Data-Broker Loophole to the Fourth Amendment's Search Warrant Requirement. *Journal of Information Security*, **15**, 589-611.
https://doi.org/10.4236/jis.2024.154033

Received: September 8, 2024
Accepted: October 26, 2024
Published: October 29, 2024

Abstract

Advances in technology require upgrades in the law. One such area involves data brokers, which have thus far gone unregulated. Data brokers use artificial intelligence to aggregate information into data profiles about individual Americans derived from consumer use of the internet and connected devices. Data profiles are then sold for profit. Government investigators use a legal loophole to purchase this data instead of obtaining a search warrant, which the Fourth Amendment would otherwise require. Consumers have lacked a reasonable means to fight or correct the information data brokers collect. Americans may not even be aware of the risks of data aggregation, which upends the test of reasonable expectations used in a search warrant analysis. Data aggregation should be controlled and regulated, which is the direction some privacy laws take. Legislatures must step forward to safeguard against shadowy data-profiling practices, whether abroad or at home. In the meantime, courts can modify their search warrant analysis by including data privacy principles.

Keywords

Access Control, Access Rights, Artificial Intelligence, Consumer Behavior, Consumer Protection, Criminal Law, Data Brokers, Data Handling, Data Privacy, Data Processing, Data Profiling, Digital Forensics

1. Introduction

This paper discusses a growing policy concern in the "data profiling loophole," where investigators can buy data online without a search warrant. Three topics converge in reviewing the data-profiling loophole: individual privacy rights, national security, and artificial intelligence. Privacy concerns are implicated when

data aggregation is beyond the limited and specific purpose of initial collection, bundled together, and sold online in data profiles. Data profiles present risks to consumers and violate privacy expectations, which impacts the legal standard for permissible search warrants under the Fourth Amendment. By purchasing data profiles in lieu of forcing a third party to relinquish the information, the government can evade the requirement of a warrant under the law regarding searches. Threat actors abroad can do the same, which is inherently hazardous to national security. Artificial intelligence is how individual data sets are combined into profiles. With the potential risks flowing from the data-profiling loophole, legislatures must protect their citizens from data misuse regardless of the actor's identity. Lawmakers should be equally concerned about exploits by domestic government agencies as foreign actors.

This article primarily explores the proper handling of data according to privacy principles derived from the U.S. Constitution and private sector laws. Data privacy, which is the informational security of every American, is a national security issue, and any future laws aimed at foreign threat actors should be broad enough to encapsulate the behavior of the domestic government.

Recommendations for future considerations include legislative action and judicial inclusion of private sector laws in search warrant analysis. Legislation could be aimed at the government, at data brokers, or at the tools of data brokers. New laws can directly limit what law enforcement can collect, what data brokers can buy and sell, and what information businesses can collect generally. To better secure data privacy, data brokers need to be regulated. In the absence of laws that are on point, other options exist for tightening the gaps in informational security that allow the data-broker loophole. In particular, courts can constrict the standard under the Fourth Amendment.

Part I of this piece explains the creation and purpose of privacy, including the sibling doctrines of data privacy and privacy under the Fourth Amendment, and it provides background on data profiling and artificial intelligence. Part II of this piece discusses how the legal loophole was created for the search requirement and the initial legislation introduced to stop it. Part III of this piece makes recommendations to close the data-broker loophole by refinement of judicial tests that embrace data privacy laws in the search warrant analysis and by adopting a data privacy per se rule. Even without express legislation, the data-broker loophole can be closed. Here is the glossary of definitions and terms:

Data profiling, or "data archeology," refers to data aggregation for analysis [1].

Person refers to an individual or entity [2].

Sensitive personal data is defined as covered personal identifiers, geolocation and related sensor data, biometric identifiers, personal health data, personal financial data, and other data [2]. Sensitive data does not include any data that is publicly available, such as in a court or government record, which is lawfully available, such as for public use or personal communications [2].

Access refers to "logical or physical access, including the ability to obtain, read,

copy, decrypt, edit, divert, release, affect, alter the state of, or otherwise view or receive, in any form, including through information technology systems, cloud computing platforms, networks, security systems, equipment or software" [2].

Bulk refers to "an amount of sensitive personal data that meets or exceeds a threshold over a set time" [2].

Surveillance capitalism is defined as "an economic system built on the secret extraction and manipulation of human data" [3].

2. What Is Privacy?

Privacy is a mythical creature. The term may signal an ideal state of reclusion, but it is also an umbrella expression for several concepts. Privacy's two most relevant contexts here are data privacy and an individual's right to be free from unreasonable searches and seizures, which the Fourth Amendment prohibits. Privacy's purpose is debatable, but some have framed it as "boundary management" [4]. Generally, privacy is concerned with empowering individuals to control their security, information, and access to their information. Privacy is also a human right, as stated in Article 12 of the 1948 United Nations Declaration on Human Rights [5].

The Constitution is the original fountain of American privacy rights. The Constitution provides several "zones of privacy" embedded in different clauses and amendments, as explained by Justice Douglas in *Griswold v. Connecticut* [6]. These provisions bridge the bodily, territorial, informational, and communications ideas of privacy found within [6]. For example, the Fourth Amendment safeguards the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures" [7]. This provision protects individuals by preventing the government, during investigations, from unreasonably trespassing on property, invading bodies, unlawfully obtaining information, and intercepting communications [6].

Privacy as a term was first conceived in a law review article in 1890 by Samuel D. Warren and (pre-Justice) Louis D. Brandeis, who defined privacy as "the right to be let alone" [8]. In the 1960s, renowned Professor Prosser then adapted the ideas of Warren and Brandeis into four common law torts [9]. These included intrusion upon seclusion, public disclosure of a private fact, depiction in a false light, and misappropriation of name or likeness [9]. In sum, privacy became a broad term for informational control, bodily integrity, territorial management, and communications protections [5]. Data privacy laws then sprung up in related economic sectors as technology became intrusive [5].

In the criminal context, privacy was shaped by Justice Brandeis in 1928, who presented his views in his dissenting opinion of *Olmstead v. United States* [10]. This iconic critique would then be adopted into law as the foundation of the test under the Fourth Amendment in *Katz v. United States* [11]. The Fourth Amendment controls search warrants as an essential aspect of criminal procedure. Traditionally, a search is presumptively unreasonable inside the home absent exigent circumstances [12]. To determine when the Fourth Amendment allows a reasonable

search outside the home, the Supreme Court, leaning on Brandeis' dissent in *Olmstead*, formulated a privacy-based approach centered on the individual [11] [13]. Absent a territorial invasion; the *Katz* test determines that a search occurs when "the government violates a subjective expectation of privacy [held by a defendant] that society recognizes as reasonable" [13]. Privacy expectations, therefore, flow from the individual's perspective and manifestation, and the test requires conditional approval by society of those expectations [13].

2.1. Data Privacy

Data privacy laws govern personal information. Data privacy has evolved into an arena of technical compliance and data security requirements, many of which are outdated swiftly after the laws are enacted. Both data privacy rights and individual privacy rights from other sources are implicated by the threats posed by unmitigated artificial intelligence and data misuse like data profiling [14]. President Biden forewarned in his Executive Order on Artificial Intelligence that "Americans' privacy and civil liberties must be protected as AI continues advancing" [14]. Privacy concerns will likely be a focus in any future legislation on the uses of artificial intelligence. Moreover, congressional appetites have recently increased for an omnibus data privacy law at the national level [15].

Data privacy protections have been in development since the 1970s with standards grounded in the "Fair Information Practices" (or "FIPs") [5]. The FIPs include the following floors: there must be a specified purpose to the data collection; collection of data must be limited to that purpose; use of the collected data must be limited to that purpose; the data must retain its quality and integrity without modification; security safeguards must be in place to protect against the data's unauthorized use or access; there must be openness in the data process; natural people have the right to participate and control their data; and there must be accountability by those that collect and process the data [5]. The FIPs guide any future acts involving data privacy. The United States has already incorporated the FIPs into major legislation but does so at the sectoral level for each industry, resulting in a patchwork of different laws [5].

The federal government is subject to the Privacy Act of 1974, which requires limited purpose and use of information [5]. Meanwhile, Europe has taken an all-encompassing approach to the General Data Protection Regulation (GDPR), which incorporates all the FIPs [5]. Moreover, this law promulgates a new suite of privacy rights [5]. European residents now have the right to access data, the right to correct, the right to erasure, the right to restrict processing of their data, the right to data portability, the right to object to all processing, the right to non-discrimination in exercising privacy rights, and the right to refuse automated processing [5]. That last right means they can reject artificial intelligence handling their data, although some exceptions carve out permissible purposes. California has embraced much of the same content in GDPR in its comprehensive legislation called the California Consumer Privacy Act (CCPA) [5]. California more recently

enacted The Delete Act, which gives Californians the right to request erasure across platforms and systems with a universal opt-out mechanism [16].

The FIPs and broader privacy rights should be enumerated in any future federal A.I. legislation, and the FIPs are the key to understanding much of what President Biden espoused in his Order on AI. Additionally, President Biden released a "Blueprint for an A.I. Bill of Rights" [17]. This prescription echoes the rights and language of the GDPR and CCPA [17]. Artificial intelligence will likely run afoul of privacy and other intangible rights, so data privacy protections will go hand-in-hand with regulating AI.

2.2. Validity of Search Warrants

Search warrants are subject to a Fourth Amendment analysis for validity in a court of law [12]. The Fourth Amendment safeguards the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures" [7]. The U.S. Supreme Court has enumerated two main tests to determine when a search occurs, requiring a warrant: the physical intrusion test and the *Katz* test [18].

The physical-intrusion test is a "simple baseline" of the Fourth Amendment, resting on property interests [18]. The government conducts a search when physically entering an area sacred to the Constitution to collect information for a police investigation [19]. "When the government physically invades personal property to gather information, a search occurs" [19]. The Fourth Amendment favors the home as "a first amongst equals," and its protections extend to the close surroundings of the home or "curtilage" [18]. This approach is intended to "draw a 'firm line at the entrance to the house,'" which "must be not only firm but also bright" [13]. Yet, if a person intends to display something openly in plain sight, a search does not occur [11].

The *Katz* test evolved as a supplement to the property-based test for areas outside the home [19]. Under a privacy-based approach, "[A] Fourth Amendment search occurs when the government violates a subjective expectation of privacy that society recognizes as reasonable" [13]. Non-trespassory collections of electronic information are subject to the *Katz* test [19]. The first prong is a subjective component manifested by the defendant, and the second prong casts a broad and objective net on whatever society at large might be willing to accept as a privacy concern [19].

A person is generally acknowledged to have a reasonable expectation of privacy in their location and movements [20]. While this expectation can be undermined by sharing the information with a third party, the sharing must be voluntary and require affirmative action on the part of the individual [21]. Additionally, while a person's reasonable expectation of privacy may be weakened by traveling on public roadways, the facts and circumstances of the police surveillance of the individual will ultimately inform whether there was a violation of an individual's privacy [22].

The Supreme Court has also formulated a standard regarding technology's

impact on privacy rights under the Fourth Amendment [13]. "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" [13]. As Justice Scalia clarified in *Florida v. Jardines*, the *Kyllo* test prohibits searches with devices not in general public use when the information could only have been obtained with a trespass and physical intrusion upon the property under the protection of the Fourth Amendment [18].

Further, in *Carpenter v. United States*, the Supreme Court narrowed the third-party doctrine, finding that individuals have a reasonable expectation of privacy in their data obtained from cellphone towers, otherwise known as cell-site location information (CSLI) [20]. As the court explained, each cellphone seeks to connect to the nearest cellphone tower by "pinging," which creates a location-based time stamp or CSLI data [20]. The Supreme Court asserted gathering historic CSLI evidence requires a search warrant because "allowing government access to cell-site records contravenes that expectation" of privacy [20]. Such data "provides an intimate window into a person's life," and the tracking of a cellphone provides "near perfect surveillance" [20]. Thus, data provided to third parties that reveal intense and intimate details would be subject to a search warrant [20]. Moreover, lower courts have held that an individual does not "forfeit the expectation his property would remain private simply because he did not erect an impregnable barrier to access" [23].

As "fruits of the poisonous tree," the exclusionary rule requires evidence gained from an unlawful search and seizure to be deemed inadmissible in a court of law [24]. In other words, if a search is defective, the evidence obtained as a result must be excluded from use at trial [25]. One day, the Supreme Court may be forced to enumerate that a search occurs when data profiling information has been bought and any resulting evidence must be excluded. Still, no such decision has yet been rendered in the loophole.

2.3. Data Profiling & Artificial Intelligence

Recently, President Biden issued data profiling directives detailing the known risks and threats that foreign actors pose to national security when they obtain such data [2]. This Executive Order sets the policy of the United States to restrict "bulk sensitive data" (BDS) from "countries of concern" [2]. While President Biden focused on foreign actors and countries, the order highlights the sensitivity of data concerning American individuals and the dangers of misuse [2].

President Biden has also issued an executive order on artificial intelligence, thereby tasking federal agencies to research and develop approaches and regulations for artificial intelligence in general public use and by the government. In his Executive Order, President Biden instructed the federal government to begin developing AI guidance, standards, and safeguards [14]. This could lead to the federal government enacting legislation to employ AI in agencies and in the courts.

Data profiling and artificial intelligence can possibly be addressed within the same legislation because data profiling utilizes artificial intelligence. Understanding how data profiling and artificial intelligence work is key to recommending related policies and solutions and the interplay with search warrants in government investigations.

2.3.1. Defining Data Profiling

Data sets are often collected, bought, and sold for consumer monitoring and "prediction analytics" [26]. "Web-scrapping" occurs when data brokers comb the internet, including social media websites, for consumer information [27]. "Behavior targeting" is the process by which companies use these profiles to advertise specialized services in accordance with the trends in the data [28]. Such information about persons and their behavior is collected by cookies from browser interactions, by spyware installed with software, and by deep packet inspection (DPI) [28]. DPI is also accomplished with software development kits rooted in downloadable applications for mobile technology [29]. As some scholars have suggested, the collection of information from wearable technology, such as Fitbits, may be even more offensive to the Fourth Amendment, because the data is even more sensitive and revealing when worn on the body, which exposes movement and intimate details like heart rate and fitness activities [30].

Location information is an attractive subset of data coveted in data profiles [31]. Location data can provide details about a person's daily commute, what stores they shop at, whose homes they visit, what doctors or clinics attend, etc [31]. Location can cater to the economic demand for Strawberry Pop-Tarts and beer before a hurricane [32]. Other types of information, such as pregnancy status, are equally appealing for retailers to target consumers with directed advertisements [33]. Some commentators refer to predictive analytics as "big data" or using artificial intelligence to analyze large data sets [33].

Police use of big data has been documented in predictive criminal assessments, mass surveillance, and DNA databases [33]. "Location intelligence" is the law enforcement use of location data [34]. Crime analysis is one use of location intelligence, and government investigators find location information helpful in identifying phones in the area of activity to sweep a pool of suspects, potentially implicating innocent bystanders [34]. At least one government agency, U.S. Customs and Border Patrol (CBP), has contracted with a data profiling firm called Venntel [34]. Venntel obtains its smartphone-user data from various sources, including ad firms and weather apps [34]. CBP has used Venntel's services to identify mobile device locations within a selected area or to identify a specific user of a device [34]. However, it is likely that the individual never intended or was aware that CBP would obtain their data this way. Indeed, American data yields hearty business for data brokers, who have no deterrent to refrain from selling to the government.

2.3.2. Defining Artificial Intelligence

Artificial intelligence is "a machine-based system that can, for a given set of

human-defined objectives, make predictions, recommendations or decisions influencing real or virtual environments" [14]. People have bandied about artificial intelligence for decades, discussing its looming ascendancy and utility [35]. Yet recently, the world has been exploding with AI chatter [36]. The animating energy from this latest wave of interest in AI radiates from the release of "generative" and "large language model" (LLM) AI for public use [36]. Generative means they spawn "fresh, new" content. As a subset of the generative family, LLMs write new textual material [36]. In practice, LLMs are fun new internet toys with risks that are yet to be fully understood. "Artificial general intelligence" (or A.G.L.), the white whale in the sea of unpublished AI research, is essentially machine thinking on par with humans [37]. However, neither A.G.L nor "Artificial Super Intelligence," which is machine thinking superior to that of humans, are the intended primary targets of the AI Executive Order [37].

All these noted AI forms belong to the genus of machine learning [37]. "Machine learning programs use mathematical formulations to perform tasks and are coded to improve their ability to perform those tasks when given additional information" [37]. Machine learning has swiftly advanced and is pushing progress across industries [37]. However, present AI technology might not yet be ready for mass utilization and is still vulnerable to serious manipulation [38]. The Federal Trade Commission (FTC) has warned that AI is riddled with design flaws, contaminated with bias and discrimination, and incentivized by "commercial surveillance creep" [39]. Additionally, specific models, like ChatGPT, have been known to "hallucinate" or manufacture inaccurate facts. An AI hallucination has also created a sexual harassment scandal, sullying the reputation of an innocent law professor.

Data profiling is becoming dependent on AI. Another type of data AI collects is biometrics, which concerns individuals' physical or biological identifying characteristics [34]. Clearview AI is a renowned aggregator of biometrics [34]. Biometric data includes facial recognition, fingerprints, iris scans, and other data obtained by authentication methods [34]. Clearview AI engages in web scraping against social network policies and often takes images [34]. At least one government agency, U.S. Immigration and Customs Enforcement (ICE), has contracted with Clearview AI [34]. This implies that the government uses AI to hunt unauthorized individuals within the United States through their sensitive biometric data. This means a disproportionate impact on immigrant communities and a clear threat to privacy and civil liberties.

Protecting privacy and civil liberties, whether from threat actors or the government, are priorities for the White House in regulating AI [14]. As President Biden cautions, "Artificial intelligence (A.I.) holds extraordinary potential for both promise and peril" [14]. Feasibly, AI can crack critical problems to beneficially create a "more prosperous, productive, innovative, and secure" world [14]. Possible risks from AI include "irresponsible use [which] could exacerbate societal harms" [14]. Law enforcement's workaround to the search warrant requirement

could be one such irresponsible use, directly impacting privacy rights. Accordingly, AI and its potential use in data profiling are whisking society into a new paradigm requiring human review and oversight to protect individual rights.

3. The Data Profiling Loophole to the Search Warrant Requirement of the Fourth Amendment

Once upon a time, in the early 2000s, Americans were distraught at the idea that large data sets about individuals could be collected to predict behavior [40]. Americans were upset that their transactional, travel, and email histories would be aggregated by data brokers and sold in data profiles [40]. But today, data profiling is a commercial mainstay, creating informational sketches of individual consumers by stringing together their online activities [41]. Personal information collection has been an ever-present tradeoff for convenient and quick technological access.

The data-broker loophole, however, should offend proponents of the Fourth Amendment. Police can avoid a search warrant analysis by purchasing select information from data brokers, who provide data profiles of consumers [42]. Meanwhile, the internet thrives on the commerce of data [42]. Consumers shed data daily, which naturally falls into third-party databases [42]. Police purchase this data in the hands of third parties, creating a "loophole" in search warrant analysis [42]. The data profiling loophole can be closed by Congress directly bundled with other legislation or tightened by judicial search warrant analysis controls.

3.1. How the Loophole Came to Be: The Creation of a Gremlin

As explained above, investigators have traditionally been required to obtain a search warrant to collect evidence when probable cause exists that a crime has been committed [11]. The Electronic Communications Privacy Act of 1986 forbids communication service providers from selling information directly to law enforcement for surveillance [33] [43]. Law enforcement has been stepping around that illegality by purchasing the information from third-party resellers, known as data brokers [44]. Data brokers do not come under the definition of covered entities under the statute [33]. Because the information is bought—and not coerced or forced from the processor—investigators have operated on the assumption that they do not offend their legal obligations for warrants [33].

In 2018, in *Carpenter v. United States*, the Supreme Court examined the issue of whether a search warrant is required to obtain cell-site location information and whether an individual has a reasonable expectation of privacy when others get their cellphone location information [20]. The Court held that an individual does have a reasonable expectation of privacy, even though the information lands in the hands of a third party [20]. Despite *Carpenter* holding that a search warrant is required to obtain such information, the information has been deemed by law enforcement not to offend the opinion, which is dubious [33].

Surveillance capitalism should be reined in, as some like the Brennan Center

for Justice have advocated [33]. Purchased profiles run the risk of racial and religious harm by law enforcement, such as tracking Muslims through prayer apps and following racial activists [33]. Additionally, abortion rights have been decimated, and some states may misuse available online reproductive health information to prosecute individuals seeking abortions [33]. These harms will increase with the proliferation of artificial intelligence, which will assist in collecting information and identifying individuals, whether by providing quicker results or a more thorough collection of data [33]. Personal data can show home or work locations, travel history, and associations [45]. The purchase of these intimate details can assist law enforcement in obtaining information that they could only obtain through dragnet operations or invasions of the home or phone, which require search warrants. Data profile purchases by law enforcement are conducted mischievously and without good faith because investigators know this is a legal loophole. The privacy rights of Americans are at risk if no action is taken. The search warrant loophole needs to be closed.

3.2. The End Is Near for the Loophole

Stopping the use of the data-profiling loophole will be challenging for legislators because the practice has become ingrained in the habits of law enforcement. As Senator Ron Wyden has warned, "If the government can buy its way around Fourth Amendment due process, there will be few meaningful limits on government surveillance" [45]. Limits could soon be imposed on data brokers by two bills on the hill if passed. Firstly, the Fourth Amendment is Not for Sale Act targets the data-broker loophole directly. Secondly, the other law is the American Privacy Rights Act, which could include the FIPs and limitations on data brokers, which have so far been outside legislation.

3.2.1. The Fourth Amendment Is Not for Sale Act: Direct Legislation Aimed at the Data-Broker Loophole

A new legislative solution is on the horizon to directly stop the police purchase of online data. In April 2024, the U.S. House of Representatives passed the Fourth Amendment is Not for Sale Act (FAINSA). This bill directly targets the data-broker loophole, which is now in the hands of the U.S. Senate [46]. The Act prohibits the government from purchasing data of Americans from data brokers, effectively ending this drama if fully enacted [46]. Of course, the data-profiling loophole is a separate concern from the warrantless searches authorized by the Foreign Information Secrecy Act (FISA), which has also just received a vote and renewal by the House in a separate bill, which addresses obtaining data of foreigners abroad and extension of the secretive FISA court [47]. Conversely, the passage of FAINSA would close the loophole as it concerns Americans and domestic use by the government.

President Biden opposes the FAINSA bill partly because it does not deal with the national security piece of sensitive information sold by data brokers to foreign adversaries [48]. President Biden also opposes the legislation because it too strictly

prohibits the U.S. government from buying "commercially available information," which is "subject to only narrow, unworkable exceptions" [48]. The President may have a valid point of contention: a blanket ban on the government may not be the ideal form of regulation. The government may have some interest and uses not intrinsically harmful in obtaining online information from data brokers. The FAINSA may be too overbroad. While closing the loophole is necessary for search warrants for the risks imposed on the average American, a thorough analysis of other alternatives may be beneficial to ensure that the proper safeguards are put in place to the right extent.

As proxy wars fueled by the advancement of technology increase online, privacy rights will likely evolve alongside national security and artificial intelligence. The rules, however, cannot be stricter for foreign adversaries than domestic actors behind an official office desk. Congressional attention must be given to the potential harm to individual rights posed by foreign threat actors, unmitigated artificial intelligence, and commercial surveillance. Personal security should become a national priority. Thus, FAINSA should also be amended to include national security concerns in sensitive information. Nonetheless, FAINSA should be passed to protect privacy rights.

3.2.2. American Privacy Rights Act: Ending the Loophole in an Omnibus Federal Data Privacy Law

As some scholars have noted, one of the best solutions to eliminating the search warrant loophole would be a national data privacy act on a broad level that encompasses this issue and more. Still, proposed legislation for an omnibus data privacy law like the GDPR has so far been a failure in Congress [26]. Nevertheless, a bipartisan bill, the American Privacy Rights Act (APRA) of 2024, gained traction in the current Congress [15] [49]. The APRA is designed to be a national data privacy rights bill, replacing and supplementing the collage of state and federal laws across sectors, with some exceptions [15] [49]. The APRA would permit Americans to universally withdraw consent from targeted advertising and empower Americans to "view, correct, export or delete their data and stop its transfer" [49]. The APRA, as written in May of 2024, would expressly preempt similar state laws [15]. In other words, Americans would be given complete control of their data [49]. Representative Cathy McMorris Rodgers promised the law would "establish privacy protections stronger than any state law on the books" [49]. APRA would also include a private right of civil action for a plaintiff to sue for harms incurred due to a data breach [50]. Should the APRA bill pass, citizen control of their data would be undeniable.

3.2.3. Stopping the Loophole with Legislation Targeting Artificial Intelligence

Many people project that the dominance of artificial intelligence will soon be achieved [51]. In response, the government may need to enact legislation to protect civil liberties and civilization very soon. Advocates of APRA suggest that an

extensive data privacy law can be enacted concurrently with a bill governing artificial intelligence this year [51]. As one such supporter commented, restricting the quantity of data available should be just as possible as restricting data on which to train AI [51]. Yet until a data privacy bill is enacted that directly targets the sale of information to and from data brokers, Congress may be more motivated to regulate the artificial intelligence industry as a steamier hot-button issue.

The best approach could be to regulate data brokers and artificial intelligence to restrain the government's behavior. Any future federal legislation addressing governmental use of artificial intelligence or data privacy could address this loophole by applying the FIPS. The collection limitation alone could stop the aggregation of extraneous data. Data brokers could be prevented from selling to anyone who is interested in the information outside of advertising as a purpose limitation, which could be tracked by AI.

Some scholars recommend state and federal experiments in "legal regulatory sandboxes" [52]. These can be testing jurisdictions that help understand and apply new AI regulations in smaller batches.

Another idea is creating a specialized AI and technology court where certified questions can be sent. Much like how appeals in patent cases are taken to the U.S. Court of Appeals for the Federal Circuit [53], a court for AI questions and appeals would promote consistency and predictability in case law, particularly under the Fourth Amendment. Specialized knowledge of judges and the staff in their chambers could be helpful for efficiency and timeliness. To engage the potential of AI in federal courts, the foundation must be solid to ensure privacy and civil rights and to protect against discrimination for natural persons.

Transparency will be essential to effectuate due process and to reduce discrimination by AI. Nevertheless, protecting individual rights must be a priority. AI could be used to monitor government collection of information, which could yield more credible evidence. Boundary management, including constitutional and statutory rights to privacy, will be a growing area of law as artificial intelligence progresses.

4. Recommendations For the Courts to Control the Government Use of Data Profiling to Search

Absent legislation fixing the loophole, other approaches may cure some of the ills stemming from the data-broker loophole. After all, the danger to civil liberties arising from foreign adversaries targeting individuals by data profiling should apply equally to domestic government agencies under a search warrant analysis. Courts should update their analysis to a new era of data privacy rights. This might be done in two general ways: by tweaking the *Katz* test or creating a new standalone rule for when a search implicates information protected by a data privacy law. The best solution to patching data profiling under the Fourth Amendment is to look how other sectors have handled intrusive technology. Search warrant analysis does not need to reinvent the wheel on how to handle privacy.

4.1. Tweaking the *Katz* Test's Flawed Approach to Reasonableness in Online Data and Technology

Some scholars and courts have critiqued the treatment of privacy under Fourth Amendment analysis after *Katz*, citing faults in two related areas: one, that privacy is deemed a "question of fact rather than a constitutional value," and two, court interpretations are deemed "out of touch with society's true expectations of privacy" [54]. Judicial guesswork about privacy and how society views privacy should not be a substitute for evidence and a prosecutor's burden of proof. The courts have at least three options to treat these blemishes: removing society as a factor, compelling a factual burden of proof, or explicitly merging privacy laws into the society analysis.

For starters, the courts could claw back the phrasing of "society would deem as reasonable" entirely and replace it with "objectively reasonable." Conceivably, this is a looser test that is unconstrained by the issue of what society believes and puts more control in the judge's hands to determine what is reasonable in an argument. With experience and wisdom, a judge may have better ideas and expectations of privacy as viewed by fiction than what society conjures up. Conversely, this puts objectivity in the judge's hands and, likely, the judge's subjective opinions. Moreover, the courts have entrusted this second prong to "society" for years and are unlikely to walk away from it.

This is a key component of the problem with the reasonable expectations standard: society may not actually be a good measure. Past decisions imply that the objective prong is what the ideal society would deem reasonable, but there is no recourse if society is misinformed or uniformly unreasonable in rationale. As here, society writ large does not understand its privacy rights and what is given in exchange for a social media login.

4.1.1. Society May Not Be Reasonable or Well-Informed

According to Pew Research, society has a cynical view about their privacy online [55]. Most Americans admit they do not understand what businesses do with their internet-generated data [55]. Many believe they have no control over their data and that their data will be sold without their consent [55]. Almost sixty percent of Americans do not bother to read privacy policies online [55]. Nearly seventy percent view privacy policies as obstacles to content [55]. One-third of white adults fear the theft of personal information or identity online, whereas almost half of Hispanic, black, or Asian adults express this anxiety [55]. Only fifteen percent of Americans are "apprehensive" about law enforcement monitoring their activities online, which drops down to ten percent for white people [55].

The Pew Research survey also targeted select points related to search warrant issues and law enforcement surveillance: older adults were far more permissive than younger adults in supporting criminal investigations into cell site location information (86% to 57%), forcing the turnover of private communications (61% to 45%), and breaking passcodes to smartphones (68% to 35%) [55]. However, these statistics do not accurately reflect all of society, nor are the views themselves

informed and reasonable. While many Americans admit they do not know what is going on with their data online and they might approve even unlawful conduct by police investigators, these stats reflect that society might not even understand their rights. These stats also need more context.

For instance, under the decision in *Carpenter*, law enforcement would require a warrant for compelling cell-site location information (CSLI) from a third party [20]. Did the poll respondents know their Fourth Amendment rights? If confronted with information on what is permissible, would their answers have changed? Of course, most Americans are unlikely to be well-versed in the nuances and perimeters of criminal procedure. The unseen actions of the internet blind society and unaware that not all access to their data is permissible according to the courts. This is why it is so curious that the specter of society is anointed with so much power under the Fourth Amendment. Add in another variable of the internet, wherein Americans admittedly do not fully understand their rights, and the supposition lifts to the surface that society cannot be a cognizant and adequate decision-maker.

Further, many Americans and even respected jurists like Judge Posner have expressed nonchalance about exposing their data online [56]. However, this attitude underestimates unguarded data's personal and commercial risks, like identity theft, harassment, and social engineering [57]. Returning to President Biden's Executive Order, if the federal government soon recognizes the risk of data misuse by spies [2], indeed, that view should override not only the straw-man's perspective but also the actual general public's understanding of data privacy risks when data profiles are sold online. The Fourth Amendment cannot be blind to privacy findings in other contexts. Therefore, courts should rethink society's preparation and acceptance of reasonableness in light of documented risks that flow from data.

4.1.2. Proving Society's Beliefs Is Becoming a Matter of Fact

Alternatively, the courts could fully submit to society's beliefs, changing the *Katz* standard to an issue of provable fact. But it should be by more than just survey evidence. A prosecutor would have to establish reasonableness in the eyes of society with valid and comprehensive evidence. Comparably, trademark law requires proof in the general public's perception of an essential element called "secondary meaning." Secondary meaning refers to marks that are not inherently distinctive and have developed as a source-identifier in the public's mind over time [58]. Courts look at objective surveys as one of five supportable factors to prove what the public thinks [58]. Other factors measure quantity and quality of the public's understandings from other evidence [58].

Applied to the search warrant requirement of willingness by society to view subjective expectations as reasonable, not many reasons come to mind to excuse the lack of evidence of what is becoming a triable issue of fact. When *Katz* was decided in 1967, accessible and practical technology likely did not exist to quantify public opinion. But nowadays, in 2024, prosecution teams must be keen to use technology in some capacity to streamline their tasks, and quantifying opinion is

within the pale of government capability. How aware society is of an issue and their attitudes towards it are far more measurable than not in the digital era.

However, this approach would likely bog down dockets and be impracticable if every search warrant suppression hearing required increased evidentiary burdens. Even further, unless a counterweight was specifically incorporated as well, the concern that the public was uninformed and unreasonable would not be ameliorated. Nevertheless, factual determinations bleeding into search warrant analysis will become even more problematic in the future.

4.1.3. *Kyllo*'s "General Use" Requirement Also Calls for Facts and Will Eventually Need Clarification

As a subset of the search warrant analysis, the *Kyllo* holding offers a refinement of the *Katz* standard, particularly in terms of technology as investigative equipment [13]. This measure is more recent and not effusively litigated yet, but courts risk dangerous precedent from an overbroad reading of "technology" and "general use" under the supplemental *Kyllo* standard [13]. For example, an iPhone is "ubiquitous" and widely used today by the general public. Yet, all potential uses of an iPhone as a smart device cannot fall under *Kyllo*'s intent. Indeed, they do not: the implied logic of the holding of *Jardines* and the express text of Justice Kagan's concurrence in *Jardines* assured that not all uses fall under the *Kyllo* standard but the particular "use" at issue [18]. But which uses do?

Some courts have already decided whether using an iPhone is acceptable as a non-search, finding on threadbare evidence that using an iPhone to see through the tinted glass of an automobile was in general use and, therefore, not an impermissible search [59]. To reach this conclusion, the court pointed to online articles that foretold thieves knew of the use to break into cars [59]. Should that be enough? Are thieves and reports about thieves sufficiently representative of the public? Likely, the Fourth Amendment did not intend illegality and threat actors to form the basis of governmental control and check on law enforcement. Whether a threat actor's behavior and abilities constitute general use could be a future issue to be decided by the Supreme Court.

Indubitably, the "general use" of technology under the *Kyllo* test will require clarity by future courts. How much the general public knows about how a device is used can likely be demonstrated through statistical analysis, such as survey evidence, which can illuminate the knowledge of the use, the length, and manner of a user's existence in the public sphere, as well as the geographic and demographic composition of the public's awareness. Other sources of proof, such as the volume of view counts on public channels, can show actual instances of knowledge of the use at issue. Moreover, technology can address society's actual beliefs in multiple ways.

Whether a "use" is within the general public's understanding should be viewed as a matter of fact to be proven by the state. However, it is doubtful that courts intended search warrant jurisprudence to devolve into trials. Nevertheless, search analyses under *Katz* and *Kyllo* bend like pretzels, advancing arguments into the

Fourth Amendment, which resemble calls for factual determinations. American courts are likely not equipped to speculate on the idiosyncrasies of all technology or devices and their perceptions fixed within the general public. Society is neither decipherable without evidence, singular in belief, nor necessarily well-informed. Future courts should reconsider the old tests and implement a new baseline to determine factual reasonableness as society and technology update.

4.1.4. Returning to Privacy's Origins for Guidance

Other scholars have advocated using Justice Brandeis' dissenting opinion in Olmstead as a baseline for privacy concerns in the face of developing technology, bringing privacy back to its roots [60]. After all, informational privacy governance in the private sector and search warrant rights in the criminal realm shared a doctrinal father in Justice Brandeis. Justice Brandeis once wrote, "Decency, security, and liberty alike demand that government officials shall be subjected to the same rules of conduct that are commands to the citizen" [10]. Criminal law, then, should be consistent with civil law on privacy. This can be extrapolated to the premise that if a data privacy law commands that certain information be kept private, law enforcement must obtain a warrant.

Because modern data privacy laws incorporate already vetted concepts and controls, the society-as-built-into-the-law approach could be an adequate gloss to the *Katz* test. While this may be a patronizing view of society as incapable of neutral and knowledgeable opinions, it still involves reasonableness and adds direction from practices established in the civil sector. Indeed, those who assemble data privacy laws are likely more informed about informational concerns than the general public. Moreover, privacy laws can support a subjective expectation of reasonableness as well. Most importantly, expectations grounded in other laws can support search warrant analysis. Noted in *Rakas v. Illinois*, property law already serves this purpose:

> *Legitimation of expectations of privacy by law must have a source outside of the Fourth Amendment, either by reference to concepts of real or personal property law or to understandings that are recognized and permitted by society. One of the main rights attaching to property is the right to exclude others, see W. Blackstone, Commentaries, Book 2, ch. 1, and one who owns or lawfully possesses or controls property will in all likelihood have a legitimate expectation of privacy by virtue of this right to exclude. Expectations of privacy protected by the Fourth Amendment, of course, need not be based on a common-law interest in real or personal property or on the invasion of such an interest [61].*

Data privacy laws reflect society's values, and the Fourth Amendment should acknowledge that. These laws also reflect academics, practitioners, and legislators who have intense interests and appetites in ensuring privacy generally. In that light, the courts can step back from emphasizing the "objective" prong of *Katz* as related to society and look more at what the law of data privacy says privacy is,

particularly across subdomains of different laws that touch on technology. After all, many privacy laws have come into existence since *Katz* was decided in 1967, *i.e.*, the Privacy Act of 1974, the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach Bliley Act (GLBA), Telephone Consumer Protection Act (TCPA), and the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM), *et al.* [5]. Indeed, many of these laws rendered deliberate considerations on technology and informational privacy. Some of these acts concern health, financial, and communication information, governing both hardcopy and internet forms of personal information. Several of these acts give specific rights to individuals regarding their personal information, such as notice, access, and consent [5]. Only the CCPA grants the right to delete, otherwise known as erasure [62]. Some laws provide private rights of action in case of data breach and misuse [5]. Data privacy rights embedded in these enactments offer individuals control of their data in the hands of third parties.

Setting the standard to reflect a search that occurs when a trespass on protected data is not an illogical leap. After all, both the Fourth Amendment and data privacy fixate on privacy and share a logical father. Considering that many data breach laws exist, alongside authorizations for enforcement actions bearing penalties and provisions providing private rights of action, Americans do have some expectations that their data will remain secure and out of the hands of illicit actors and malicious misuse. Imaginably, an approach enveloping data privacy laws would be fairer to a defendant than an uninformed and unreasonable society, whose existence and opinion are a matter of conjecture. Law enforcement efforts would also be supported because generally publicly available information that is affirmatively and voluntarily shared by an individual would still be fair game and consistent with data privacy laws. Additionally, tethering a search to information protected under data privacy would draw a bright line.

4.1.5. Proposing the "PII Per Se" Rule

The courts should adopt a new test, the personally identifiable information (PII) per se rule. Courts should declare that a search occurs when an officer obtains information protected from disclosure by privacy laws and the data is not otherwise publicly available. The query then must turn to which data sets are protected and by which laws.

Yet, absent an omnibus federal law, many data laws are currently inconsistent in their definitions of protected data. Sensitive data is often acknowledged as requiring additional layers of protection, but sensitive data is not universally defined. For example, some statutes include biometric or genetic information as personally identifiable information (PII). In contrast, many others do not, and this is largely a function of outgrowth as the statutes have not caught up to the concepts as technology rages on.

To compensate for the uneven landscape in the realm of data privacy, the best practices have been to observe the broadest understanding to mitigate risk flowing from data and compliance liability. In other words, the strictest law demands the

most attention and receives the most respect. But suppose a universally accepted definition of protected personal information were to be enacted in a federal privacy law, such as APRA, as discussed earlier. In that case, a court should have no problem accepting congressional findings that this information is as worthy a basis, much like property law.

This test could stand alone, as *Katz* protects intangible and transient privacy and does not displace property-based interest analysis [18]. After all, the Fourth Amendment protects people, not places [11]. The Fourth Amendment, however, does not say how and in which way it protects people, beyond their persons, houses, papers, and effects, from unreasonable searches and seizures. Data should be protected as "papers" within the understanding of the Constitution since so much information has moved online, and the digital world has replaced the physical copy. Using the FIPs and laws like the CCPA as guidelines for a judicial test could be the answer to data collection limitations, ensuring data is not misused by overbroad police investigations and securing data of individual Americans. These privacy practices likely will be added to any omnibus data privacy law. Including consideration of the FIPs in search warrant analysis makes sense.

Furthermore, including data privacy laws in the search warrant analysis is consistent with the "legitimation" principles mentioned in *Rakas*, as quoted above. Because property law provides a basis to determine when a search occurs chiefly due the right to exclude others from that property, then an individual with the right to control their data, including the right to prevent others from using or selling it, should enjoy that same respect from the Fourth Amendment.

Notably, it is the existence of the property right to exclude and not whether an individual did in fact tell any police officer to stay out of his house that makes an intrusion upon the home and its immediate surrounding areas per se unreasonable. Unconsented entry is presumed to be offensive. Unconsented secondary handling of data should also be assumed to be offensive. Individuals can control their data under some privacy laws; therefore, Americans have the right to exclude others from obtaining their data under those laws. The Fourth Amendment should see the existence of control in data privacy rights as analogous to the existence of property rights. If the American Privacy Rights Act or its equivalent is ever enacted to give Americans complete control of their data, this view should strengthen.

On the other hand, a flaw might be the treatment of consent. Consent to disclose data is provided under murkier waters than consent to entry in property law. Because Americans do not see the invisible intrusions to intangible data, because they may not understand to what they are consenting, and because there is no guarantee that the party provided the data is complying with any limitations on that consent absent strict regulations, consent should not be the basis for which to determine if a search occurs.

Nevertheless, the PII per se rule could provide an easy guideline for determining a bright line. As favored by Justice Scalia, bright lines in criminal procedure

are helpful for law enforcement and courts alike [13]. Under a PII per se rule, privacy expectations would be presumed, as would reasonableness. The burden of proof would then shift to the government as a rebuttable presumption to show that the information was obtained lawfully within compliance with data privacy laws. This showing could then require the government to prove they received the information in good faith, whether commercially or publicly available. Yet, whether such a PII per se rule would only apply to online informational privacy may be a matter of debate because some data privacy laws also include physical recordings of stored information.

Likely, there will be many more quirks to iron out with search warrant analysis. While the courts can refine search warrant practice through the judicial process, a decision by the Supreme Court to change the standard nationally may take several, if not many, years. Nevertheless, it is time for courts to observe the expectations preserved in data privacy laws corresponding to the same principles entrenched in the Fourth Amendment. After all, Justice Brandeis promoted privacy in both the civil and the criminal realms during his lifetime. The genesis of privacy springs from one source, and the courts should treat data privacy laws as an equal, if not superior, source for Fourth Amendment "legitimation" over property law. Once data privacy is entrenched in the federal code, a PII per se rule could be a much better measure for search warrants for future generations.

5. Conclusion

Modern search warrant requirements may be devolving in utility. While criminal law may be particularly behind in adaptation to technology, many aspects of technology have already been vetted in the private sector. While the average American may need to better assess cybersecurity and data privacy risks, professionals assembled these laws about privacy concerns. Easy access to personal information puts individuals at risk from threat actors abroad and the government. Personal identity can serve as a source of vulnerability for Americans. Currently, that vulnerability is manifesting in the data-broker loophole. If Congress does not enact the Fourth Amendment is Not for Sale Act, it must do more to protect American civil liberties. Should Congress disappoint, the courts need to fine-tune the search warrant analysis to accommodate those failings. The courts may need to adjust their standards regardless. The current test for whether a search has occurred has already grown tired and worn. As technology advances, so must the law.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] IBM. What Is Data Profiling? https://www.ibm.com/topics/data-profiling

[2] Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern, Exec. Order No. 14117, 89 Fed.

Reg. 15429, 15421-22, 15428-29 (Mar. 1, 2024).

[3] Rahnama, H. and Pentland, A.S. (2022) The New Rules of Data Privacy. *Harvard Business Review*. https://hbr.org/2022/02/the-new-rules-of-data-privacy

[4] Cohen, J.E. (2013) What Privacy Is for. *Harvard Law Review*, **126**, 1904-1905.

[5] Swire, P. and Kennedy-Mayo, D. (2020) U.S. Private-Sector Privacy: Law and Practice for Information Privacy Professionals. International Association of Privacy Professionals, 3, 2, 219, 21, 43, 391, 398-402, 147, 42-44, 4-7, 177-178.

[6] Griswold v. Connecticut, 381 US 479, 484 (1965).

[7] The Fourth Amendment Protects Individuals from Unreasonable Searches and Seizures. U.S. Const. Amend. IV.

[8] Warren, S.D. and Brandeis, L.D. (1890) The Right to Privacy. *Harvard Law Review*, **4**, 193-220. https://doi.org/10.2307/1321160

[9] Prosser, W.L. (1960) Privacy. *California Law Review*, **48**, 383-423. https://doi.org/10.2307/3478805

[10] Olmstead v. United States, 277 U.S. 438, 478, 485 (1928) (Brandeis, J., Dissenting).

[11] Katz v. United States, 389 U.S. 347, 351 (1967).

[12] Payton v. New York, 445 U.S. 573, 586-90 (1980).

[13] Kyllo v. United States, 533 U.S. 27, 33, 40 (2001).

[14] Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, Exec. Order No. 14110, 88 Fed. Reg. 75191, 75193 (Quoting 15 U.S.C. § 9401(3)), 75191-93, 75196 (Oct. 30, 2023).

[15] Congressional Research Service (2024) The American Privacy Rights Act. CRS Reports. https://crsreports.congress.gov/product/pdf/LSB/LSB11161

[16] CPPA Applauds Governor Newsom for Approving the California Delete Act (2023) California Privacy Protection Agency. https://cppa.ca.gov/announcements/2023/20231011.html

[17] Blueprint for A.I. Bill of Rights: Making Automated Systems Work for the American People. The White House. https://www.whitehouse.gov/ostp/ai-bill-of-rights/

[18] Florida v. Jardines, 569 U.S. 1, 5, 6-7, 11 (2013); Id. at 12 (Kagan, J., Concurring).

[19] United States v. Jones, 565 U.S. 400, 409-14 (2012).

[20] Carpenter v. United States, 585 U.S. 296, 311 (2018).

[21] Smith v. Maryland, 442 U.S. 735 (1979).

[22] United States v. Knotts, 460 U.S. 276 (1983).

[23] People v. Camacho, 3 P.3d 878, 885 (Cal. 2000).

[24] Wong Sun v. United States, 371 U.S. 471, 488 (1963).

[25] United States v. Leon, 468 U.S. 897, 906 (1984).

[26] Reid, C. (2024) The Fourth Amendment Covers "Fog Reveal": Not the Other Way Around. *Wake Forest Journal of Law and Policy*, **14**, 127, 128, 142.

[27] Doktor, M. (2020) Facial Recognition and the Fourth Amendment in the Wake of Carpenter v. United States. *University of Cincinnati Law Review*, **89**, 552, 555.

[28] Berger, D.D. (2011) Balancing Consumer Privacy with Behavioral Targeting. *Santa Clara Computer and High Technology Law Journal*, **27**, 3, 6-7.

[29] Stemler, A. (2022) Privacy & Antitrust Reform: How to Avoid the Starfish Problem. *Notre Dame Law Review Reflection*, **97**, 417-429.

[30] Rodis, A. (2020) Fitbit Data and the Fourth Amendment: Why the Collection of Data

from a Fitbit Constitutes a Search and Should Require a Warrant in Light of Carpenter v. United States. *William and Mary Bill of Rights Journal*, **29**, 533, 551.

[31] Thompson, S. and Warzel, C. (2019) Twelve Million Phones, One Dataset, Zero Privacy. *The New York Times*. https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html

[32] Joh, E.E. (2014) Policing by Numbers: Big Data and the Fourth Amendment. *Washington Law Review*, **89**, 35-68.

[33] Ayoub E. and Goitein, E. (2024) Closing the Data Broker Loophole: Congress Must Pass Legislation That Prohibits Government Agencies from Buying Its Way around the Fourth Amendment and Other Legal Privacy Protections. Brennan Center for Justice. https://www.brennancenter.org/our-work/research-reports/closing-data-broker-loophole

[34] Shenkman, C., Franklin, S.B., Nojeim, G. and Thakur, D. (2021) Legal Loopholes and Data for Dollars: How Law Enforcement and Intelligence Agencies Are Buying Your Data from Brokers. Center for Democracy and Technology, 23, 24, 11, 34.

[35] Surden, H. (2014) Machine Learning and Law. *Washington Law Review*, **89**, 87.

[36] Heilweil, R. (2023) What Is Generative AI, and Why Is It Suddenly Everywhere. Vox. https://www.vox.com/recode/2023/1/5/23539055/generative-ai-chatgpt-stable-diffusion-lensa-dall-e

[37] Wang, M. (2023) Use of Artificial Intelligence (AI) in the Field of Law. *Arizona Law Journal of Emerging Technologies*, **6**, 1, 4-5.

[38] Stokel-Walker, C. (2023) Jailbroken AI Chatbots Can Jailbreak Other Chatbots: AI Chatbots Can Convince Other Chatbots to Instruct Users How to Build Bombs and Cook Meth. Scientific American. https://www.scientificamerican.com/article/jailbroken-ai-chatbots-can-jailbreak-other-chatbots/

[39] Federal Trade Commission (2022) FTC Report Warns about Using Artificial Intelligence to Combat Online Problems: Agency Concerned with AI Harms Such as Inaccuracy, Bias, Discrimination, and Commercial Surveillance Creep. Federal Trade Commission. https://www.ftc.gov/news-events/news/press-releases/2022/06/ftc-report-warns-about-using-artificial-intelligence-combat-online-problems

[40] McClurg, A.J. (2003) A Thousand Words Are Worth a Picture: A Privacy Tort Response to Consumer Data Profiling. *Northwestern University Law Review*, **98**, 63-144.

[41] Kuempel, A. (2016) The Invisible Middlemen: A Critique and Call for Reform of the Data Broker Industry. *Northwestern Journal of International Law and Business*, **36**, 207-234.

[42] Clifton, A. (2022) Privacy, Network Effects, and Law Enforcement: The Gap between Technology and the Law. *Seattle Journal for Social Justice*, **21**, 213, 217, 218, 220-221.

[43] The Electronic Communications Right Act, 15 U.S.C. § 9401(3).

[44] Guariglia, M. (2024) Fourth Amendment Is Not for Sale Act Passed the House, Now It Should Pass the Senate. Electronic Frontier Foundation. https://www.eff.org/deeplinks/2024/04/fourth-amendment-not-sale-act-passed-house-now-it-should-pass-senate

[45] Gallagher, R. (2023) Legal Loopholes Help US Spies Buy Americans' Personal Data: Such Information Can Be Used for an Array of Purposes, a Key Report Has Found.

Bloomberg.
https://www.bloomberg.com/news/newsletters/2023-06-21/legal-loopholes-help-us-spies-buy-americans-personal-data

[46] Schilke, R. (2024) House Ends FISA Saga with Passage of Fourth Amendment Is Not for Sale Act. Washington Examiner.
https://www.washingtonexaminer.com/news/house/2969992/house-fisa-saga-passage-fourth-amendment-not-for-sale-act/

[47] Savage, C. and Broadwater, L. (2024) House Passes 2-Year Surveillance Law Extension without Warrant Requirement. *The New York Times*.
https://www.nytimes.com/2024/04/12/us/politics/surveillance-bill-fisa.html

[48] Executive Office of the President (2024, April 16) Statement of Administration Policy, H.R. 4639—Fourth Amendment Is Not for Sale Act (Rep. Davidson, R-OH, and Seven Cosponsors).

[49] House Energy and Commerce Committee (2024) Spokesman Review: Cantwell, Rodgers Strike Bipartisan Deal on Landmark Data Privacy Bill. House Energy and Commerce Committee.
https://energycommerce.house.gov/posts/spokesman-review-cantwell-rodgers-strike-bipartisan-deal-on-landmark-data-privacy-bill

[50] Smith, O.D. (2024) Cantwell, McMorris Rodgers Strike Bipartisan Deal on Land-Mark Data Privacy Bill. *The Spokesman Review*.
https://www.spokesman.com/stories/2024/apr/07/cantwell-mcmorris-rodgers-strike-bipartisan-deal-o/

[51] Anderson, J. and Rainie, L. (2018) Artificial Intelligence and the Future of Humans. Pew Research Center.
https://www.pewresearch.org/internet/2018/12/10/artificial-intelligence-and-the-future-of-humans/

[52] Simshaw, D. (2023) Toward National Regulation of Legal Technology: A Path Forward for Access to Justice. *Fordham Law Review*, **92**, 1, 7.

[53] United States Courts (2020) Just the Facts: Intellectual Property Cases-Patent, Copyright, and Trademark. United States Courts.
https://www.uscourts.gov/news/2020/02/13/just-facts-intellectual-property-cases-patent-copyright-and-trademark

[54] McKelvey v. State, 474 P.3d 16, 27 (Alaska Ct. App. 2020) (Quoting 1 Wayne R. Lafave, (2012) Search and Seizure, § 2.3(g), at 799-800).

[55] McClain, C., Faverio, M., Anderson, M. and Park, E. (2023) How Americans View Data Privacy: The Role of Technology Companies, AI and Regulation—Plus Personal Experiences with Data Breaches, Passwords, Cybersecurity and Privacy Policies. Pew Research Center.
https://www.pewresearch.org/internet/2023/10/18/how-americans-view-data-privacy/

[56] Lin, W.C. (2016) Where Are Your Papers: The Fourth Amendment, the Stored Communications Act, the Third-Party Doctrine, the Cloud and Encryption. *DePaul Law Review*, **65**, 1093, 1135-1136.

[57] Opderbeck, D.W. (2022) Cybersecurity and Data Breach Harms: Theory and Reality. *Maryland Law Review*, **82**, 1001. https://doi.org/10.2139/ssrn.4187263

[58] Security Center, Ltd. v. First National Security Centers, 750 F.2d 1295, 1298-1301 (5th Cir. 1985).

[59] United States v. Poller, No. 3:22-CR-165 (JAM), 2023 WL 4535338, at *5 (D. Conn. July 14, 2023).

[60] Kerr, O.S. (2004) The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution. *Michigan Law Review*, **102**, 801-888. https://doi.org/10.2307/4141982

[61] Rakas v. Illinois, 439 U.S. 128, 143 n. 12 (1978).

[62] Lyon, C. and Myers, J. (2023) California's Delete Act Could Be Next Frontier beyond CCPA. Bloomberg Law News. https://news.bloomberglaw.com/us-law-week/californias-delete-act-could-be-next-frontier-beyond-ccpa