Section 6. Political science

https://doi.org/10.29013/EJHSS-22-6-81-92

Dai Raymond

THE RIGHT TO INFORMATION DATA PRIVACY ON THE INTERNET

Abstract. This paper examines why individuals lack data privacy on the Internet, and it does so by exploring the ways in which constitutional and statute law fail to provide adequate privacy protections – even when rights to privacy are intended. As the author argues, there are "three main reasons for the scarcity of Internet data privacy: first, the law lacks a sufficient definition of data privacy. Second, existing laws and statutes regarding the right to data privacy have inherent flaws and loopholes. Third, the modern era of web design is inconvenient for users and leads to an unfair engagement of contracts, which in turn, gives users little choice but to expose their data to third parties.

Keywords: Right to privacy, Right to data privacy, Information privacy, Consumer privacy, Fourth Amendment, Fourteenth Amendment, Griswold v. Connecticut, Roe v. Wade, Search and Seizure, Katz v. United States, Olmstead v. United States, Privacy Act of 1974, Securities and Exchange Commission, Federal Trade Commission, Facebook, Google, Consumer Privacy Bill of Rights, General Data Protection Regulation, California Consumer Privacy Act.

The right to privacy is not specifically enumerated in the United States Constitution as a guaranteed right of the people, as the Bill of Rights and other amendments have done such as with the freedom of speech or the right to bear arms. The closest clause suggesting a right to privacy appears in the Fourth Amendment [37]. The right to privacy is still a fairly novel concept, as its first notable mention only appears in Samuel D. Warren II and Justice Louis Brandeis's "The Right to Privacy", a *Harvard Law Review* article published in 1890. In it, Warren and Brandeis advocate for a right to privacy, or more specifically, "the right to be left alone" [30].

In June 2022, the U.S. Supreme Court overturned the constitutionally guaranteed right to abortion care established in its 1973 decision *Roe v. Wade*. In the 2022 decision overturning *Roe, Dobbs v. Jackson Women's Health Organization*, the right to reproductive rights is now decided among the states. However, the right to privacy does not extend only to reproductive rights; questions concerning the right to privacy also pervade the digital world. The internet is still less than thirty years old, as the inception of the World Wide Web by computer scientist Tim Berners-Lee began in 1989. Since then, the internet has seen an unprecedented era in the explosion of both social networking around the world and the sharing of convenient access to information technology. From 2000 to 2016, the World Wide Web has grown from 413 million global users to 3.4 billion [20]. At the same time, these developments have allowed private technology companies and

websites to gather information about individuals either unknowingly or without their consent. As early as 2001, "Web bugs" tracked the sites people visit and send the information to third-party marketing research and advertising companies, which, in turn, are now used on 18 percent of web pages [31]. Another report found that it was possible for websites to make freely available individual voter's registration records along with their home addresses on the Internet [16].

This paper examines why individuals lack data privacy on the Internet today. It pinpoints three main reasons for the scarcity of Internet data privacy: first, the law lacks a sufficient definition of data privacy. Second, existing laws and statutes regarding the right to data privacy have inherent flaws and loopholes. Third, the modern era of web design is inconvenient for users and leads to an unfair engagement of contracts, which in turn, gives users little choice but to expose their data to third parties.

The lack of a concrete definition of data privacy can lead to loose interpretations of any right to data privacy. In the event of a case challenged in the Supreme Court, one's right to personal information would likely not fall under Fourth Amendment privacy protections. Instead, as technology continues to develop over time, the Supreme Court would more likely favor security over privacy [32]. This is mainly because of the Fourth Amendment's particular phrasing–it only forbids "unreasonable searches and seizures." However, the words "seizure" and "searches" are loosely defined and have been set only by Supreme Court precedents.

The Supreme Court defined "seizure" as the interference "with anyone's possessory interest in a meaningful way" in the 1984 *United States v. Karo* [42] the Court ruled that the Drug Enforcement Administration (DEA) did not violate the right to one's possessory privacy when it installed beepers inside cans to monitor and detect ether that was moved around among the respondents' homes and to commercial storage lockers. A government informant had told DEA agents that respondents Karo, Horton, and Harley had ordered 50 gallons of ether from them for the use of extracting cocaine from clothing imported into the United States. After executing a warrant to search the house based on information gathered by the beeper, law enforcement seized cocaine and arrested Horton, Harley, Steele, and Roth. While Rhodes contended that a warrant was required to install the beeper in the ether can in the first place and that the warrant for searching Horton, Harley, and Steele's rented house was tainted by the government's prior illegal conduct, the Supreme Court argued that because the can containing the beeper conveyed no private information pertaining Karo, it did not substantially interfere with anyone's possessory interest.

The precedent was further upheld by the Court's 1987 decision in *Arizona v. Hicks* [3]. After a bullet fired through the floor of an apartment wounded a man below, police searched the apartment for the shooter, victims, and weapons, but also stumbled upon stereo components. The police suspected that the stereo components were stolen and recorded the serial numbers and phoned them to headquarters along with moving some components and a turntable. Subsequently, the police found that the turntable had been taken during an armed robbery and seized it. The Arizona Court of Appeals held that the policeman's obtaining of the serial numbers had violated the Fourth Amendment because the seizure was unrelated to the shooting incident and did not justify the entry and search. However, the U. S. Supreme Court ruled that copying serial numbers did not constitute a seizure, as recording the numbers did not affect the respondent's possession of the numbers or stereo equipment. This trend continued in *Bills v. Aseltine* [4], in which the United States Court of Appeals for the Sixth Circuit ruled that taking photographs of a search scene was not a seizure.

Yet, one exception to the trend persists. In the 1967 *Katz v. United States* case [18], FBI agents wiretapped a petitioner's telephone call and introduced the electronic listening and recording device attached

outside the telephone booth in which Katz had made calls at a trial. Katz was convicted for transmitting wagering information by telephone across state lines, violating U. S. Code 18 Section 1084, which the Court of Appeals upheld and found no Fourth Amendment violation because the FBI did not physically enter the telephone booth. In response, the Supreme Court rejected the ruling, claiming that the government violated the petitioner's right to privacy while using the telephone booth as the Fourth Amendment protects people rather than places and extends to recording oral statements.

As a result of these Supreme Court rulings, it is unlikely that copying a user's computer files containing personal information would ever be protected under a court of law in the United States' highest judicial body because possession of such files containing conversations or credentials would allow for one to control the use of information inside of it while possessing a physical item used to communicate such as a stereo would interfere with one's use of the device. It is possible to search through one's personal records and information without touching computer equipment at all. Thus, defendants may lack standing to challenge illegal searches of private information, as limited by the Supreme Court. Still, because personal data ultimately lies closer to a written document or oral conversation, it could be protected under the Fourth Amendment and its subsequent protections.

The definition of the word "search" in a Fourth Amendment context is even more difficult to define than "seizures." In fact, the Supreme Court has never given a comprehensive definition of what the word means under the Fourth Amendment at all [44]. Instead, before 1967 and *Katz*, cases such as *Olmstead v. United States* [22] pointed towards an area-based definition of "search."

In 1928, government officers secretly wiretapped a telephone line and intercepted a conversation between the accused, who had conspired to violate Prohibition [35]. The use of this evidence in a federal court was deemed not a violation of the Fifth Amendment right to not self-incriminate, and the Supreme Court also ruled in *Olmstead* that because the tapping connections were made on public streets in a large office building's basement and not on the property of the defendants, there was no violation of the Fourth Amendment.

As mentioned above, *Katz* sharpened an individual's expectation of privacy and focused it on individuals instead of certain areas. Justice John Harlan's concurring opinion has since laid out the standard of a "search" under two conditions: first, that the individual exhibits an expectation of privacy, and second, that the expectation of privacy is deemed reasonable by society [43]. Nevertheless, this standard of privacy remains uncertain and tenuous because the government can defeat it relatively easily. The definition of an expectation of privacy remains unclear and largely under this loose interpretation, and statute laws cannot completely or accurately account for the variety of ways an individual infers privacy. On the other hand, the government can announce its intentions of surveillance in advance and completely subvert these expectations.

Second, a "reasonable" expectation of privacy is just as subjective, as it merely reflects the extent to which a society honors a right to privacy, and the Supreme Court has interpreted this idea as whether or not an individual expects to be undisturbed, as seen in *Rakas v. Illinois* [27]. In *Rakas,* a 1978 decision, police stopped robbers who were leaving the scene of a crime and seized a box of rifle shells and a sawed-off rifle. Prosecutors admitted the items as evidence in an Illinois court to convict the robbery suspects. In this case, the U. S. Supreme Court reasoned that the defendants did not have Fourth Amendment rights because they failed to demonstrate a legitimate expectation of privacy in the car as passengers. However, this reasoning limits the defendants' right to privacy by burdening them with proving their expectation of privacy; instead, the question of reasonableness ought to shift to the methods police use to investigate criminal suspects.

Because of these flaws in the current definition of the right to privacy, there is currently little use in applying the Fourth Amendment in the context of data privacy; individuals would either have the absolute right or none at all. It is also important to understand that the Fourteenth Amendment [36] does not protect data privacy either–the constitutionally protected "zone of privacy" is evident in two spheres: independence in making personal decisions and the independence to avoid disclosing personal matters. Justification of the constitutional right to privacy upheld by the 1965 *Griswold v. Connecticut* [15] case and *Roe v. Wade* [29] using the Fourteenth Amendment only applies to the personal sphere, not the latter; the extent of one's right to avoid disclosing personal matters has not yet been defined by the Supreme Court [33].

Aside from the vague definition of an expectation of privacy, current legislation has multitudes of inherent flaws, loopholes, and poor implementation, which leads to a failure of upholding the right to information privacy as intended. For example, in *Nixon v. Administrator of General Services* [21], the Supreme Court in 1977 articulated a right to information privacy, yet never developed this concept further. Because of this, there is no authoritative definition of the right to information privacy; the Court leaves the matter up for debate to lower court jurisdictions.

The Privacy Act of 1974 [26] established regulations for the collection and use of records by the federal government, and individuals have the right to access and correct their personal information. This legislation did make a step in controlling government information systems, but it also has crucial shortcomings. One important problem with the act is that it does not apply to the private sector at all, and it does not apply to state or local governments either, only the federal government.

Furthermore, personal information may still be disclosed for a "routine use" exception, if doing so is considered "compatible" with an agency collecting the information's purpose. This "routine use" exception effectively serves as a loophole that can be used to completely avoid obliging under the Privacy Act [23]. While the Privacy Act of 1974 also attempted to restrict the use of Social Security Numbers (SSNs), these rules once again did not apply to the private sector. In the present-day world, SSNs are now used as a form of a password for individuals to access personal records at banks, schools, and hospitals.

Weaknesses in the federal regulation of one's right to privacy only precede the widespread collection of Internet users' personal information by private technology companies. One of the most straightforward reasons private technology companies can ignore consumer data privacy rights is simply because they illegally collect and share data from users.

In September 2019, Google agreed to pay a $170 million settlement after the Federal Trade Commission (FTC) and the New York Attorney General filed a complaint that Google's YouTube video-sharing service illegally collected information from children without consent from their parents [10]. This was a violation of the 1998 Children's Online Privacy Protection Act (COPPA) [5], which requires that child-directed websites and online services notify users of their information practices and privacy policies prior to collecting personal information for children under 13 years of age with parental consent. Such methods of identifiers include tracking a user's Internet browsing habits to sell for targeted advertising and third-party advertising networks. YouTube had marketed itself as a top online destination for children yet had not complied with the necessary regulations.

Even though the $170 million settlement was the largest sum of money gathered by the FTC by a COPPA case, Google's parent company, Alphabet, earned a profit of $30.7 billion off of $136.8 billion in revenue collected from targeted advertising alone in 2018 [28]. Thus, many lawmakers and children's advocacy groups argue that the repercussions are extremely light for these private technology conglomerates.

One of the most famous incidents of the illegal sharing of data occurred in 2018 when an online leak

found that Facebook, the world's largest social media platform with approximately 3 billion monthly active users [7], had been providing the personal information of over 80 million profiles for the purpose of political advertising without users' consent to Cambridge Analytica, a political consulting company connected to President Donald Trump [38]. For the egregious breach of consumer data privacy rights, Facebook was punished with a $5 billion penalty by the FTC; while this was the largest regulatory penalty imposed by the United States government on a company, many criticized the fine because it did not impose any meaningful change to the company's structure or financial incentives, leading to no change in the underlying reason for the data scandal in the first place. Instead, some commissioners advocated for litigation against Facebook and Zuckerberg [8]. Years after the incident, Facebook remains a prominent company that still generates billions of dollars in revenue without many concrete restrictions, despite the magnitude of the Cambridge Analytica scandal. Monetary fines in response to consumer privacy data scandals will continue to receive backlash if structural changes are not implemented as well, which the United States government must be responsible for enacting on private technology companies.

In the status quo, there is no expectation of confidentiality or privacy online for Internet users due to the widespread tracking of online activity without permission. Thousands of websites use canvas fingerprinting, allowing them to track users' activity on the Internet without informing them, and the usage of cookies also enables websites to track users' activity and display targeted and invasive advertisements based on identified consumer preferences and can reveal sensitive information about the user. In addition, individuals downloading mobile apps on their phones can grant mobile application companies access to a plethora of cell phone features and data [17].

When private technology companies amass control of such large quantities of personal information, the databases are often subject to breaches or compromises. One of the most notable examples arose in the 2018 Marriott International hacking, in which hackers breached its Starwood reservation system and stole the personal data of up to 500 million of its customers [24]. This breach affected customers who made reservations in subservient Starwood hotel brands from 2014 to 2018, including Sheraton, Westin, W Hotels, St. Regis, Four Points, Aloft, Le Méridien, Tribute, Design Hotels, Element, and the Luxury Collection. While the Residence Inn and Ritz-Carlton hotels operated on a separate reservation system, Marriott International had planned to merge those systems with Starwood, which would have put even more customers at risk of having their personal information exposed had it been done before the instance of the data breach. Stolen personal credentials included names, addresses, phone numbers, birth dates, email addresses, and encrypted credit card details, as well as travel histories and passport numbers for a smaller group of guests. Not only that, but the security breach went unnoticed for four years; it started in 2014 when a security tool alerted officials to an unauthorized attempt to access the guest reservation database, which also led to the discovery of a foothold gathered by hackers in Starwood's systems. Since the data breach, Marriott International has offered one year of free enrollment in Web Watcher, a service in the United States, Canada, and Britain that tracks websites where thieves exchange and sell personal information and alerts users if their information is being sold.

Another significant data breach incident pertains to Equifax, an American credit reporting agency that reported in September 2017 that a data breach exposed the personal information of 147 million people and resulted in the theft of credit card and driver's license info, birth dates, SSNs, and addresses [11]. The company agreed to a $425 million settlement with the FTC, the Consumer Financial Protection Bureau, and 50 U.S. states and territories to help the victims of the data breach. Equifax has also offered free credit monitoring for those who filed claims for settlement benefits.

Even if only one private technology company unlawfully gathers the data of its customers, that personal information can be and is often compromised in the form of data breaches, which can spread the credentials far and wide across the Internet into the hands of malicious actors without any means of retrieving the data back to its source.

Modern web design practices continue to perpetuate a lack of data privacy among consumers, as all responsibility is left to them to control their own personal information when allowing private technology companies to do what they wish with it is the much more convenient option.

As current laws stand, private technology companies follow the "informed consent" model, a practice used in medical care and human subject research, where consumers encounter privacy notices and privacy policies online as they use the Internet [19]. However, because of the massive explosion in Internet usage since the inception of informed consent in the 1990 s, informed consent – which would require consumers to read through privacy policies written in legalese from every single website they visit on the Internet is no longer practical. Because of this, a majority of adult Americans today, or 97 percent polled by the Pew Research Center, have been asked to agree to privacy policies at least once when using the Internet, yet a very small minority of 22 percent of polled adult Americans always or often bother to read the entire fine print and only 13 percent understand what these policies entail [25]. Along with these statistics comes the fact that only 21 percent of polled adult Americans are very or somewhat confident that private companies will publicly admit mistakes and take responsibility if they misuse or compromise users' personal data, suggesting little public confidence in private companies' accountability with their personal information.

Systematic changes can be made to remedy many of the issues present with current data privacy practices. The first change pushed by data privacy advocates is the opt-in system, where personalized data collection is allowed only through this system with transparency and conciseness. Removing unnecessary and long legal text that the average American would never read paves the way for a truly consensual individualized targeting of users by private technology companies or political campaigns [47].

Secondly, providing individuals access to all the data a private company has gathered about them, as well as computational inference, or information on how the company uses the gathered data to extrapolate personal preferences, personal and medical history, political ideologies and more can provide an additional level of transparency for the general public [39].

Third, another method to further empower consumers' control over their personal information on the Internet is by specifically enumerating the timeframe in which collected data can be used. Limiting data harvesting to an expiration date creates more proper regulation on the duration of time of harvesting an individual's personal information.

Fourth, the aggregate use of data can be regulated. Even if private technology companies claim that individuals will own their data, there still exists the possibility of convincing people to give away personal information for an aggregate level, such as if a private company were to gather health information on a billion customers, which can still create unforeseen threats to individuals and public harms [41].

Despite claiming to value information privacy as among their key values, social media users are often quick to assume that private technology companies will look after their best interests and thus sign agreements giving away their right to informational privacy. In reality, this is not the case; many companies may end up taking advantage of this lack of knowledge and privacy rights until the event of an incident. As social media users continue to post large volumes of personal information, most simply hope that businesses will make moral decisions and keep their customers informed of changes.

As of now, the presence of monopolies in the technology industry exacerbates the lack of account-

ability in private technology companies. Because Facebook Meta's products are used by billions of consumers worldwide, individuals lack the power to singlehandedly ask Facebook to change its privacy policy practices. Alternatives including Snapchat or a potential new non-profit service provided by Wikimedia and funded by the Corporation for Public Broadcasting do exist [46], but they can be smaller and not as practical to switch to compared to staying with the current service.

Two existing pieces of legislation outline a potential solution to the lack of regulation of data privacy practices by private technology companies: the Obama administration's Consumer Privacy Bill of Rights and the European Union's General Data Protection Regulation. Both texts outline a set of basic rights that consumers have on the Internet with regard to data privacy.

The Consumer Privacy Bill of Rights enumerates seven key protections for consumers: individual control, transparency, respect for context, security, access and accuracy, focused collection, and accountability [40]. The bill requires the FTC to establish a set of rules regarding the collection of personal information in order to increase consumer privacy [6]. Under the Consumer Privacy Bill of Rights, consumers have greater control over their personal information, as private technology companies that gather data must notify individuals of how their personal information is used in an easily understandable and accessible format, obtain express approval to use a consumer's personal information and provide the ability to withdraw that approval. The companies cannot deny service based on a refusal to approve the collection of their personal information nor can they offer price incentives in exchange for approval. The companies must ensure that depersonalized information cannot be restored to make an individual identifiable, and not disclose personal information to a third party under a written contract unless the contract prohibits the third party from using the personal information for any other reason than performing the contracted service or disclosing the personal information to another third party.

Consumers also have the right to secure and responsible handling of their personal information; they can access, correct in case of inaccuracies, or delete personal data upon request. They also have a reasonable limit on the personal data that companies collect and retain, as well as appropriate measures to ensure that private technology companies will handle personal information while adhering to the Consumer Privacy Bill of Rights. Until the proposal of the Consumer Privacy Bill of Rights, these specific data privacy rights were never enumerated before by laws or statutes in the United States.

In the European Union, the General Data Protection Regulation (GDPR), put into effect on May 25, 2018, is a strict privacy and security law for people in the EU, which levies heavy fines of tens of millions of euros against those that violate its privacy and security standards [45]. The law's foundations are based upon the 1950 European Convention on Human Rights, which states that all people have the "right to respect for his private and family life, his home and his correspondence" [9]. As technology continued to develop, the EU passed the European Data Protection Directive in 1995, which established minimum data privacy and security standards, and each member state based its own implementing law.

Similarly to the Consumer Privacy Bill of Rights, the GDPR outlines seven protection and accountability principles: lawfulness fairness and transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality, and accountability [14]. The processing of personal information must be lawful, fair, and transparent. Data that is processed must be used for the explicitly stated purpose of collection. Only the necessary data that is needed for the specified purposes may be processed. Personal data must be accurate and up to date and may only be stored for as long as necessary for the specified purpose. Processing personal information must ensure security, integrity, and

confidentiality with methods such as encryption. Finally, private technology companies or entities processing personal information must demonstrate compliance with all principles of the GDPR.

Accountability can be achieved in several different manners. A team may designate data protection responsibilities, maintain detailed documentation of the collected data of how it is used, where it is stored, and which employee is responsible for it, train staff and implement technical and organizational security measures, have Data Processing Agreement contracts with third parties to process data, or appoint a Data Protection Officer, to name a few.

Data security is handled by implementing "appropriate technical and organizational measures," which can include two-factor authentication for accounts with stored personal data and contracting with cloud providers that use end-to-end encryption. Organizational measures may include staff training, a data privacy policy as a part of an employee handbook, and access to personal data limited to only employees who need it. Data breaches must be reported within 72 hours, or private technology companies or entities will face penalties unless technological safeguards such as encryption can render leaked personal information useless to an attacker. Everything done by an organization must consider data protection from the very beginning in designing any new product or activity.

Under the GDPR, processing personal data is legal, but only under a few conditions. These conditions include the individual granting specific and unambiguous consent to processing the data (such as opting into a marketing email list), collecting personal data to enter into a contract, background check, a legal obligation required by a court, performing a task in the public interest, or when there is a "legitimate interest" that is not overridden by an individual's "fundamental rights and freedoms" [14]. If the situation does not apply to one of the aforementioned conditions, an individual's personal data should not be collected, stored, or sold to advertisers. Afterward, the instance must be documented, and the individual must be notified for transparency. The same process applies to a change in justification.

Consent from a consumer to process their personal information must be "freely given, specific, informed and unambiguous," distinguishable in "clear and plain language," and recorded with documentary evidence of consent [13]. Data subjects can always withdraw previously given consent, in which the decision must be honored, and children under the age of 13 may only give consent with parental permission. Since its passage in 2015, the GDPR has also prompted companies in the United States to embrace more privacy-friendly practices. Amazon has promised to strengthen encryption around its stored data from cloud storage services and give customers the right to choose which region they would like their data to be stored [2].

While the Consumer Privacy Bill of Rights may prove to be more adaptable to evolving technology such as artificial intelligence, which may require aggregate masses of data for machine learning or smart infrastructure than the rigid GDPR, ultimately both the draft and law create strong foundations for a more secure and transparent Internet where users can feel safer and more confident in how their personal information is gathered and processed, if at all.

New data privacy regulations are in the works or being implemented rapidly in the United States. In 2018, the State of California passed the California Consumer Privacy Act (CCPA), which secured new privacy rights for its consumers, including "The right to know about the personal information a business collects about them and how it is used and shared; The right to delete personal information collected from them (with some exceptions); The right to opt-out of the sale of their personal information; and The right to non-discrimination for exercising their CCPA rights" [34]. Businesses are required to disclose the personal information they collect on consumers, including the purposes for which it is to be used, the categories of third parties with whom

the business shares the personal information, and the categories of information that the business sells or discloses to third parties. While there are more exceptions in the CCPA that allow for businesses to retain an individual's personal information, one may still request to have it deleted by the business and for it to tell its service providers to do the same.

With regards to the right to opt-out of sale, consumers may request businesses to stop selling her personal information and cannot do so upon receiving the opt-out request unless authorization allowing them to do so again is provided. There is a 12-month period until businesses can ask to opt back into the sale of personal information. Children under the age of 13 cannot opt-in at all without approval from a parent or guardian.

There are no punishments for exercising one's rights under the CCPA. Businesses cannot deny goods or services, charge different prices, or provide a different level of quality of goods and services. However, refusing to provide personal information to a business or asking to delete or stop selling it may prevent it from completing a transaction if the use of that personal information is necessary for it to provide goods and services. Businesses are allowed to offer promotions, discounts, and deals in exchange for collecting, keeping, or selling personal information, but this is only allowed if the financial incentive is reasonably related to the value of the individual's personal information. Individuals may not be able to participate in these special deals offered in exchange for personal information if they ask a business to delete or stop selling their personal information.

The right to privacy, as Mark Alfino and Randolph Mayes of the Florida State University Department of Philosophy explain, is a fundamental moral right that must be upheld in order to uphold personal autonomy and liberty [1]. With respect to informational privacy and the "right to be left alone," there are currently many barriers preventing individuals from accessing this right in the online sphere, as private technology companies continue to routinely abuse the lack of regulations of data privacy to profit by selling personal information for targeted advertising or other third parties. While some individuals may be willing to share their personal information with private technology companies, it is crucial that they are fully aware of the implications and precise details of what they are sharing, and these companies must take on the role of a "fiduciary," or prioritizing a client's interests over its own. There are already steps being taken to secure this right for individuals as seen by the Consumer Privacy Bill of Rights, GDPR, and CCPA, but it is important to understand how we arrived at this situation in the first place. Only when legislation supported by the highest levels of the judicial system is passed, is void of loopholes and shortcomings, and holds private technology companies or entities accountable for their actions can people finally begin to take back control of their right to information privacy.

References:

1. Alfino Mark and Randolph Mayes G. "Reconstructing the Right to Privacy." Social Theory and Practice,– 29 (1): 2003.– P. 1–18. URL: https://www.jstor.org/stable/23559211.
2. Amazon Web Services, Inc. "GDPR – Amazon Web Services (AWS)." 2018. Accessed: October 17, 2022. URL: https://aws.amazon.com/compliance/gdpr-center
3. Arizona v. Hicks, 480 U.S. 321 (1987).
4. Bills v. Aseltine, 958 F.2d 697, 707 (1992).
5. Children's Online Privacy Protection Act of 1998, 15 U.S.C. 6501–6505
6. Congress.gov. "S.1214–116th Congress (2019–2020): Privacy Bill of Rights Act". April 11, 2019. Accessed October – 10. 2022. URL: http://www.congress.gov

7. Datareportal. "The Latest Facebook Stats: Everything You Need to Know." DataReportal – Global Digital Insights. Accessed: October 10. 2022. URL: https://datareportal.com/essential-facebook-stats
8. Davies Rob and Dominic Rushe. "Facebook to Pay $5bn Fine as Regulator Settles Cambridge Analytica Complaint." The Guardian. The Guardian. July 24, 2019. Accessed: October – 10. 2022. URL: https://www.theguardian.com/technology/2019/jul/24/facebook-to-pay-5bn-fine-as-regulator-files-cambridge-analytica-complaint
9. European Court of Human Rights. 1950. "European Convention on Human Rights." Accessed October – 10. 2022. URL: https://www.echr.coe.int/Documents/Convention_ENG.pdf
10. Federal Trade Commission. "Google and YouTube Will Pay Record $170 Million for Alleged Violations of Children's Privacy Law." September 3. 2019. Accessed: October – 10. 2022. URL: https://www.ftc.gov/news-events/news/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations-childrens-privacy-law
11. Federal Trade Commission. "Equifax Data Breach Settlement." Federal Trade Commission. July 11, 2019. Accessed October – 10. 2022. URL: https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement
12. GDPR.eu. "Art. 6 GDPR – Lawfulness of Processing." 2018. November – 14. 2018. Accessed: October 17. 2022. URL: https://gdpr.eu/article-6-how-to-process-personal-data-legally
13. GDPR.eu. "Art. 7 GDPR – Conditions for Consent – GDPR.eu." 2018. November 14, 2018. Accessed October 17. 2022. URL: https://gdpr.eu/article-7-how-to-get-consent-to-collect-personal-data
14. GDPR.eu. 2019. "GDPR Archives – GDPR.eu." GDPR.eu. 2019. Accessed October 10, 2022. URL: https://gdpr.eu/tag/gdpr
15. Griswold v. Connecticut, 381 U.S. 479. (1965).
16. Harmon Amy. "As Public Records Go Online, Some Say They're Too Public." The New York Times, August 24, 2001, sec. New York. Accessed October – 10. 2022. URL: https://www.nytimes.com/2001/08/24/nyregion/as-public-records-go-online-some-say-they-re-too-public.html
17. Identity Management Institute. "6 Reasons Why Data Privacy Is Dead." 2019. September 7, 2019. Accessed October – 10. 2022. URL: https://identitymanagementinstitute.org/6-reasons-why-data-privacy-is-dead
18. Katz v. United States, 389 U.S. 347. (1967).
19. Kerry Cameron F. "Why Protecting Privacy Is a Losing Game Today-and How to Change the Game." Brookings. Brookings. July 12, 2018. Accessed October 10. 2022. URL: https://www.brookings.edu/research/why-protecting-privacy-is-a-losing-game-today-and-how-to-change-the-game
20. Murphy Julia, Max Roser and Esteban Ortiz-Ospina. "Internet." Our World in Data. 2018. Accessed: October – 10. 2022. URL: https://ourworldindata.org/internet
21. Nixon v. Administrator of General Services, 433 U.S. 425. (1977).
22. Olmstead v. United States, 277 U.S. 438. (1928).
23. Paul M. Schwartz, Privacy and Participation: Personal Information and Public Sector Regulation in the United States, 80 Iowa Law Review.– 553. 1995.– P. 585–86. URL: https://lawcat.berkeley.edu/record/1115037/files/fulltext.pdf
24. Perlroth Nicole, Amie Tsang and Adam Satariano. "Marriott Hacking Exposes Data of up to 500 Million Guests." The New York Times, November – 30. 2018. Accessed: October – 10. 2022. URL: https://www.nytimes.com/2018/11/30/business/marriott-data-breach.html

25. Pew Research Center: Internet, Science & Tech. "4. Americans' Attitudes and Experiences with Privacy Policies and Laws." Last modified November – 15. 2019. Accessed: October – 10. 2022. URL: https://www.pewresearch.org/internet/2019/11/15/americans-attitudes-and-experiences-with-privacy-policies-and-laws
26. Privacy Act, 5 U.S.C. § 552a. (1974).
27. Rakas v. Illinois, 439 U.S. 128. (1978).
28. Review of Alphabet Inc. Form 10-K for the Fiscal Year Ended December 31, 2018. 2019. U.S. Securities and Exchange Commission. Washington, D.C. 20549: United States Securities and Exchange Commission. URL: https://www.sec.gov/Archives/edgar/data/1652044/000165204419000004/goog10-kq42018.htm
29. Roe v. Wade, 410 U.S. 113. (1973).
30. Samuel D. Warren and Louis D. Brandeis. "The Right to Privacy". Harvard Law Review,– Vol. 4.– No. 5.– Dec. 15. 1890.– P. 193–220. URL: https://www.jstor.org/stable/1321160
31. Schwartz John. "Technology; 'Web Bugs' Are Tracking Use of Internet." The New York Times, August – 14. 2001. sec. Business. Accessed October – 10. 2022. URL: https://www.nytimes.com/2001/08/14/business/technology-web-bugs-are-tracking-use-of-internet.html
32. Sergent Randolph S. "A Fourth Amendment Model for Computer Networks and Data Privacy." Virginia Law Review,– 81(4). 1995.– P. 1184–1189. URL: https://doi.org/10.2307/1073541
33. Solove Daniel. "Part of the Law Commons Recommended Citation Daniel J. Solove, a Brief History of." 2006. Information Privacy Law in PROSKAUER on PRIVACY. URL: https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2076&context=faculty_publications
34. State of California Department of Justice. "California Consumer Privacy Act (CCPA)." State of California – Department of Justice – Office of the Attorney General. October – 15. 2018. Accessed: October,– 10. 2022. URL: https://oag.ca.gov/privacy/ccpa
35. The Eighteenth Amendment of the United States Constitution (Prohibition): "After one year from the ratification of this article the manufacture, sale, or transportation of intoxicating liquors within, the importation thereof into, or the exportation thereof from the United States and all territory subject to the jurisdiction thereof for beverage purposes is hereby prohibited."
36. The Fourteenth Amendment of the United States Constitution: "All persons born or naturalized in the United States, and subject to the jurisdiction thereof, are citizens of the United States and of the State wherein they reside. No State shall make or enforce any law which shall abridge the privileges or immunities of citizens of the United States; nor shall any State deprive any person of life, liberty, or property, without due process of law; nor deny to any person within its jurisdiction the equal protection of the laws."
37. The Fourth Amendment of the United States Constitution: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."
38. The New York Times. "Facebook Says Cambridge Analytica Harvested Data of up to 87 Million Users," April 4, 2018. Accessed: October – 10. 2022. URL: https://www.nytimes.com/2018/04/04/technology/mark-zuckerberg-testify-congress.html
39. The New York Times. "Tech Giants Brace for Europe's New Data Privacy Rules". January – 28. 2018. Accessed: October – 17. 2022. URL: https://www.nytimes.com/2018/01/28/technology/europe-data-privacy-rules.html

40. The White House. Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promiting Innovation in the Global Digital Economy. 2012. February 2012. URL: https://obamawhitehouse.archives.gov/sites/default/files/privacy-final.pdf
41. Tufekci, Zeynep. "Opinion | We Already Know How to Protect Ourselves from Facebook." The New York Times, April 9. 2018. sec. Opinion. Accessed October – 10. 2022. URL: https://www.nytimes.com/2018/04/09/opinion/zuckerberg-testify-congress.html
42. United States v. Karo, 468 U.S. 705, 712–13. (1984).
43. Upheld by Smith v. Maryland, 442 U.S. 735. (1979) and California v. Ciraolo, 476 U.S. 207 (1986).
44. Wayne R. LaFave, Search and Seizure § 2.1(a) (2d ed. 1987 & Supp. 1994).
45. Wolford Ben. "What Is GDPR, the EU's New Data Protection Law?" GDPR.eu. European Union. November – 7. 2018. Accessed: October – 10. 2022. URL: https://gdpr.eu/what-is-gdpr
46. Wu Tim. "Opinion | Don't Fix Facebook. Replace It." The New York Times, April – 3. 2018. sec. Opinion. URL: https://www.nytimes.com/2018/04/03/opinion/facebook-fix-replace.html.
47. Zittrain Jonathan. "Opinion | Mark Zuckerberg Can Still Fix This Mess." The New York Times, April – 7. 2018. sec. Opinion. Accessed October – 10. 2022. URL: https://www.nytimes.com/2018/04/07/opinion/sunday/zuckerberg-facebook-privacy-congress.html