The Legal Defense and Decay of Online Privacy

On the morning of September 11th, 2001, American Airlines Flight 11 and United Airlines Flight 175 departed Logan Airport within fifteen minutes of each other, both en route to Los Angeles. By the end of the hour two more planes took off, American Airlines Flight 77 from Washington Dulles International Airport and United Airlines Flight 93 from Newark International, both en route to California as well. At 8:46 a.m. Flight 11 was flown into the North Tower of the World Trade Center. Seventeen minutes later, Flight 175 crashed into the South Tower, caught on camera while media and bystanders were already reeling from the first attack. At 9:37 a.m. Flight 77 crashed into the western facade of the Pentagon, and at 10:03 a.m. Flight 93 was grounded in a field outside of Shanksville, Pennsylvania. In the aftermath of these crashes, 2,977 Americans passed and more than 6,000 others were wounded. To this day, the now infamous 9/11 Terrorist Attacks are the single largest loss of life in an act of terror, on American soil no less.

In the wake of these attacks, Congress and President George W. Bush hastily penned and signed the PATRIOT Act: an unprecedented piece of legislation that expanded the government's capabilities with regards to surveillance, interdepartmental investigations, and security procedures. Passed through the Senate with only a single "nay" vote, the PATRIOT Act has since come under scrutiny for the legal capabilities it provides law enforcement and government agencies regarding individual privacy and personal monitoring thereof. While the usage of such capabilities can, and has, led to the disruption of numerous terrorist plots without a single injured citizen between them, civilians and policymakers alike have taken keen notice of the potential for abuse in the far-reaching provisions laid out within the act, particularly with regards to the freedom of agencies to conduct wiretapping and solicitation of internet records without a court order. At the time of its induction, these functions were a modest concern (enough so that only 66 congressmen voted "nay" when it was passed through the House of Representatives), but poses a greater risk of privacy violation today due to the ever-expanding and increasingly complex web of technology the world has found itself stuck in.

However, privacy legislation is not solely limited to the PATRIOT Act. In fact, it is merely the top of the abyss pertaining to the threat to online privacy the world is finding itself sinking into as technology advances, with legislation lagging behind such. Alongside the PATRIOT Act are the decades old Electronic Communications Privacy Act (ECPA, 1986) and the Foreign Intelligence Surveillance Act (FISA, 1978), both of which were significantly amended by the PATRIOT Act itself to further their capabilities. Despite these legislations, there have been attempts and significant rulings to preserve

privacy, with the most recent and relevant being the California Consumer Privacy Act (CCPA, 2018) that gives California residents the rights and capabilities to require companies to reveal the information being kept on record of them, as well as to delete and request that such information is not sold. To this extent, the state of privacy rights online is a turbulent one that is subject to the whims of legislation and court rulings, giving way to both defense and decay of such in equal parts.

With regards to the decay of privacy rights, the textbook legislation pointing to such is found in the aforementioned PATRIOT Act. In this piece of legislation, government agencies are given the explicit go-ahead to perform unwarranted searches of personal records from private organizations including "financial records, medical histories, Internet usage, bookstore purchases, library usage, travel patterns, or any other activity that leaves a record."[8] In this case, government officials aren't required to implicate any foreign influence on the individual they are investigating, a requirement previously defined by FISA. Similarly, these same officials don't have to indicate any reasonable suspicion of the individual, much less any "probable cause" as required by the Fourth Amendment. As quite clearly evident, these provisions within the PATRIOT Act indicate a wide variety of options available to federal officials to monitor and acquire information on private citizens at any whim they may have, utterly undermining the concept of privacy on the internet on the basis of any investigation that may occur. In a similar manner, the provisions dedicated to preventing abuse of these capabilities of government agencies defined in FISA, which sought to maintain that these actions could only be taken on individuals if they were reasonably suspected to be acting foreign agents, were significantly overhauled and, in some cases, completely thrown out in the PATRIOT Act to provide officials the means to investigate anyone at any point. As a result of these provisions, along with the requirements defined in Communications Assistance for Law Enforcement Act (CALEA, 1994) for telecommunications companies to cooperate with officials in electronic surveillance efforts, online privacy continuously erodes as these legislations begin to show their age. This is particularly shown in the aspect of increased record keeping and impact of digital footprints as the world becomes more and more interconnected over the worldwide web, whereby federal investigators have their pick of the litter regarding information to analyze and record on any particular person. Furthermore, the PATRIOT Act provides significant abilities to federal agencies to conduct unregulated wiretapping which, previously, required the same level of authorization from courts as other search warrants necessitated as according to the Supreme Court ruling in *Katz v. United States* (1967). Although this ruling was watered down in the enactment of FISA in 1978 to allow for greater wiretapping capabilities by the federal government, the provisions inside FISA required suspicion of foreign allegiance for the suspected party, which was further disintegrated by the

PATRIOT Act to justify wiretapping for any individual an agency may have interest in. At the time of the Act's conception, this was simply attributed to telephone calls and voicemails. Since then, however, it has been used to tap video calls over IP providers (such as Skype, Zoom, etc.) and emails. To this extent, the law continues to lag behind technology, as these forms of communication differ greatly and exceed the anticipation of the PATRIOT Act's original jurisdiction. In this regard, the information collected and reviewed by federal officials can range from browsing history to even physical travel by means of social media postings and travel app history. As such, the capabilities of government agencies to monitor individuals causes the illusion of privacy to be quite quickly sundered, and the reality of a potential surveillance state is realized.

Unfortunately, the decay of online privacy is not limited solely to the capabilities of government bodies, but by those of private companies as well. In this case, private bodies have the ability and right to retain relevant information to their functionality as they deem to be necessary. In other cases, these private bodies also have state or federal requirements to maintain such data in the event government officials need such for a legal investigation. This data collection comes in various shapes and forms, ranging simply from placing cookies on your device to track your history and browsing access, with examples being Facebook tracking your log in so you can interact with their respective widgets on other sites to Google allowing you to remain signed in on all of their owned and operated websites, to running targeted ads based on your interaction with emailed links from retailers. The further concerning detail regarding this collection of information is how such information is shared and even sold by the holders, with particular examples of the former being PayPal confirming that they share personal information with hundreds of global entities to facilitate transactions including, but not limited to, "name, address, phone number, date of birth, IP address, bank account information, recent purchases." [13] With regards to the latter, companies selling retained data typically do so to third-party brokers, that then work with larger corporations, with the most common buyers being credit agencies seeking to get an understanding of an individual's online shopping habits and credit history. While legally sound, this sequence of events is clearly concerning to a private individual as their personal information is not only being provided to groups they have no affiliation with, but also that companies are making a profit off of their mere browsing history that gives significant insight into their actions and expectations as a person. In a sense, the retaining of such information is analogous to the collection and distribution of a person's identity across various outlets without their knowing consent, even if a privacy policy is agreed upon by the user. This concept of private collection and distribution of personal information, alongside

government information collection legislation and procedures, indicate a significant decay in one's overall privacy on the internet that becomes more entangling by the day.

However, there have been significant attempts to defend online privacy, particularly by means of recent legislation and court rulings in favor of consumer privacy. The most clear-cut example of this defense can be found in the very recent passing of CCPA in 2018, which provides a variety of rights to California residents to take back control of their personal information from private entities. For starters, under CCPA Californians are allotted the right to know what information is being collected from any business and how said information is being used and/or shared, as well as the right to have any collected data deleted by these same businesses. These two provisions working in tandem provide private individuals significant power over otherwise untouchable groups that have overarching power to collect and dispense personal information at their own behest. In particular, by being able to keep private entities in check of the information being collected by checking what they are collecting and subsequently requesting deletion, individuals can completely shut down the operations discussed previously, namely the sharing and selling of their information to other entities. Furthermore, these entities liable to accountability aren't limited solely to California based entities, but instead any for-profit entity that does any business whatsoever in California, which, given the cross-borders nature of the internet, essentially implicates any for-profit online entity that meets the broad requirements of the legislation. While this doesn't include smaller organizations, it accounts for the most grievous offenders that have more capability of monitoring and recording than those that don't fit the legislation's parameters. However, one important note regarding CCPA is that its provisions don't apply to government agencies, only those in the private sector, thus leaving individuals still fully at the mercy of federal supervision and surveillance. Finally, businesses may deny requests to know and/or delete information as discussed by CCPA if doing so would violate any security requirement their corporation may have, as well as any federal requirement for information withholding. Despite these weaknesses in the legislation, CCPA still functions as a monumental baseline for privacy protection online in the corporate sector, as it allows consumers to take back control of most of their personal information being collected, shared, and sold by otherwise unaffiliated groups.

In a similar manner, various court rulings with regards to surveillance have provided much needed clarification to the discussion of privacy legislation. One important example can be found in the ruling by the Supreme Court in *Carpenter v. United States* (2018), a case regarding cell phone tracking through location records, which resulted in a 5-4 decision concluding that search warrants were, in fact,

required in order to access an individual's location information collected from a cell phone. Prior to this ruling, the prevailing interpretation of this situation was that, by voluntarily sharing information to a third party (in this case, the cell phone service an individual registers with) the user waives their right to privacy and, as a result, allows investigators the legal standing to conduct searches without warrants. As a result of this ruling, this theory has been thrown out and instead replaced by one that can be extended to the realm of the internet, as the previously discussed theory had similarly been applied to individuals registering for internet use through an Internet Service Provider (ISP). While this decision doesn't prevent private companies from amassing significant amounts of consumer information, nor the ability of government agencies from acquiring the same information in emergency scenarios (i.e. kidnapping or other imminent danger), it does hamstring the excessive abuse of the system brought about by the signing of the PATRIOT Act. According to Chief Justice Roberts in the decision, this ruling also does not call into question the use of other means of security surveillance, such as cameras, neither does it account for "other collection techniques involving foreign affairs and national security."[9] Instead, Chief Roberts stated that it will act to "ensure that the progress of science does not erode the Fourth Amendment"[9] and its role in the realm of privacy. Finally, and most importantly, this ruling extends all rights presented under the Fourth Amendment to personal information collected digitally, rather than being subject to interpretation based on decades old laws that have since had their intention eclipsed by reality and the development of technology therein. In doing so, the Supreme Court has set the precedent that these older laws designed for physical searches can no longer be simply extended to the complex world of digital information, but instead must be modified to account for such going forward.

Despite a majority ruling in favor of requiring search warrants for investigation of cell phone records, the narrow decision indicates the varying degree of interpretation of privacy and the Fourth Amendment. A perfect example of this is indicated in the dissenting opinion penned by Justice Kennedy, who stated that "cell site records are created, kept, owned and controlled by cell phone service providers, who even sell this information to third parties."[9] In this regard, Justice Kennedy draws from the previous theory aforementioned, in that an individual cedes away their rights to privacy regarding their personal information once they give the right to a private group to collect and attribute information to their person. Under this previous theory, it can be extrapolated that ownership of such information is no longer in the hands of the individual, but in the company recording such, which can further be expanded upon to legitimize the sale of such information to third-party groups. This was further echoed by Justice Thomas, who stated that, under the Fourth Amendment, individuals do have the right to be secure from searches, however the property of the information in question fell solely in

the hands of the company rather than the individual. To this extent, these dissenting opinions offer a strong indication to the majority opinion, as inverting the interpretation of the dissenting opinions can in turn present the context that the personal information in question is now determined to belong to the individual instead of the company creating and collecting such.

In a similar manner, the constitutionality of surveillance and the PATRIOT Act itself can be brought into question under the context of such Supreme Court rulings. For example, opponents of the PATRIOT Act seek to invalidate such by arguing that its procurement violates a person's right to be secure in their effects against "unreasonable" searches and seizures. In this interpretation, opponents indicate that government access of personal information without reasonable suspicion of wrongdoing or foreign allegiance is wholly unconstitutional, as doing so invalidates a person's right to the contrary. Similarly, the precedent set by *Roe v. Wade* (1973) further indicates that a person's privacy is protected under the Fourth Amendment, thus cementing the concept of personal information being a protected entity through the Constitution. On the other hand, and as indicated by the dissenting opinions of Justices Kennedy and Thomas in the *Carpenter v. United States* case, this information could instead be interpreted to be under the jurisdiction of the company that creates, collects, and records such information, rather than the persons for which the information is maintained. Under this interpretation, which has been since stricken down by the majority ruling in the same case, the constitutionality of the PATRIOT Act is upheld as these searches are done under the compliance by the private company in control of such data as it belongs to them specifically. Unfortunately, only one case has made it to the Supreme Court that fell under the jurisdiction of the PATRIOT Act, *Holder v. Humanitarian Law Project* (2010), which simply upheld the portion of the Act that prevented material support of terrorist groups, even if such support was under the intent of teaching such groups non-violent methods of reaching their goals. To this extent, the Supreme Court hasn't officially ruled on the constitutionality of the Act's surveillance provisions, with the only major ruling upon such being found in a 2004 ruling by a judge for the US District Court for the Southern District of New York, which argued that the Act's demand for financial records from companies was unconstitutional. This argument was founded upon the fact that this section of the PATRIOT Act prevents any level of judicial challenge, as the government isn't required to indicate a specific need for the information. Despite this ruling, the dissenting opinions of Justices Kennedy and Thomas, and even the precedent set by the *Carpenter v. United States* ruling, the constitutionality of surveillance is still a grey area open to case-by-case interpretation without proper guidance by the Supreme Court regarding how to interpret such universally.

However, across the Atlantic Ocean, privacy has been greatly protected as a result of the passing of the General Data Protection Regulation (GDPR, 2016) in the European Union's territories. Underneath GDPR, European Union citizens are provided the following rights with regards to their personal information online: the right to be informed, the right of access, the right to rectification, the right to erasure, the right to restrict processing, the right to data portability, the right to object, and rights in relation to automated decision making and profiling. These rights are more or less self-explanatory, but the options they provide EU citizens is much less so. In particular, EU citizens are now fully capable of having information collected on them presented, rectified of any issues there may be, and even request the deletion of such from company records, all of which a company must comply with or face severe penalties. This so-called "right to be forgotten" is particularly intriguing due to the power it puts in the hands of private individuals regarding their data, and was specifically used, along with many of the other provisions in GDPR, as a basis to formulate the previously mentioned CCPA. Outside of these explicit rights, the GDPR further goes on to delegate storage limitations to companies (i.e. a company cannot keep personal data longer than needed, which must be justified if questioned) and requirement of appropriate security measures for protection of personal data being collected. In short, the GDPR provides a sweeping set of regulations that hold private entities accountable to personal information being held, maintaining that these entities must operate ethically, securely, and transparently with regards to the individuals in their systems.

Furthermore, despite being a foreign law to any individuals outside of the European Union, the requirements for private entities regulated by the GDPR can act as an extension of the privacy rights allotted by GDPR to all individuals by means of Virtual Private Networks (VPN's). At their most basic level, VPN's are simply means by which a user can tunnel their personal connection through an existing private server at another location, which affords the connecting user the same security afforded the server being connected to. In this manner, VPN's typically need to have both browsing and connection logs, which remains the case in the United States. However, under GDPR guidelines VPN's based in EU nations are legally required to delete all browsing logs for connected users, as holding these would constitute withholding of personal data without prior consent. Likewise, connection logs are also open to deletion upon request by users, similarly provisioned under GDPR, although withholding such information is perfectly legal by VPN operators due to the fact that these logs are secured and encrypted, as well as allowing VPN's to operate in general as they provide operators necessary information regarding customers connecting to their private network. In doing so, any international citizen that connects to a VPN with servers hosted in the European Union will benefit from the privacy

rights that respective citizens already have, thus providing a clever option for computer savvy individuals to expand their rights and options.

In a similar manner, VPN's in the United States are not legally required to collect and maintain connection nor activity logs, although Internet Service Providers are. While this does not indicate that United States VPN providers don't necessarily collect logs, as many do so that they can sell collected information to third-party groups much like the previously discussed sites, but instead functions to give providers the marketing option to provide their services without customer concern over privacy invasion. Despite this, the requirement of the federal government for ISP's to maintain connection and activity logs partially crushes these aspirations, as individuals are still fully monitored up to the point they connect to a VPN, which could serve to be evidence of potential wrongdoing if investigated by authorities. These requirements also stem from the aforementioned Communications Assistance for Law Enforcement Act, as ISP's fall under the defined jurisdiction of such and, as a result, forces such providers to accommodate the records necessary to support any investigation put forth by government agencies. As such, while one can derive significant benefits from connecting to VPN's, both domestically and internationally, United States citizens are still unable to completely skirt the federal government's capabilities of monitoring their personal information due to the role ISP's play in the overall connection framework.

As the development of ever-increasing connectivity by means of advancing technology marches on, one can easily find the existing law lagging behind such. As it was tragically found as a result of the September 11th attacks and the legislation that quickly followed them, shortsighted changes are subsequently made in emotional heights to attempt to prevent such an event from occurring ever again. In the passing of the PATRIOT Act and the subsequent renewal of the provisions within it, the United States continues to find itself fighting legal battles with its own citizens over the interpretation of its statutes and the Constitution itself. While the Supreme Court has provided significant defense of privacy in their rulings, along with their staunch interpretation of the Fourth Amendment to extend a right to privacy to all citizens, as technology continues to grow in its interconnectivity across the globe such precedents become less and less applicable to certain individual cases. To this extent, legislation itself is necessary in order to prevent each individual case from necessitating a Supreme Court ruling, with the California Consumer Privacy Act (following in the footsteps of the European Union's GDPR) seeking to take a step in the direction of greater individual control over personal information being collected by private groups. While this legislation explicitly states that it does not address the rights of government

officials to conduct surveillance on one's personal data, CCPA harkens to a brighter future of individual privacy, safety, and security on the web. Going forward, one can hope for further legislation in line with CCPA, GDPR, and the Supreme Court's ruling in *Carpenter v. United States* in order to properly secure and establish the liberties expected by the Constitution and its citizens in the digital age.

Works Cited

[1] Baig, Anas. “Why Do VPNs Need To Be GDPR Compliant?” *Infosecurity Magazine*, 6 July 2018, www.infosecurity-magazine.com/opinions/vpns-gdpr-compliant/.

[2] “California Consumer Privacy Act (CCPA).” *State of California - Department of Justice - Office of the Attorney General*, 20 July 2020, oag.ca.gov/privacy/ccpa.

[3] “Electronic Surveillance.” *Legal Information Institute*, Legal Information Institute, www.law.cornell.edu/wex/electronic_surveillance.

[4] “FAQ: What You Need to Know About the NSA's Surveillance Programs.” *ProPublica*, www.propublica.org/article/nsa-data-collection-faq.

[5] “Guide to the General Data Protection Regulation (GDPR).” *ICO*, ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/.

[6] Morgan, Andrew. “The Patriot Act and Civil Liberties.” *Jurist*, 20 July 2013, www.jurist.org/archives/feature/the-patriot-act-and-civil-liberties/.

[7] *The Foreign Intelligence Surveillance Act of 1978*, 19 Sept. 2013, it.ojp.gov/privacyliberty/authorities/statutes/1286.

[8] “Surveillance Under the USA/PATRIOT Act.” *American Civil Liberties Union*, www.aclu.org/other/surveillance-under-usapatriot-act.

[9] Totenberg, Nina. “In Major Privacy Win, Supreme Court Rules Police Need Warrant To Track Your Cellphone.” *NPR,* 22 June 2018, www.npr.org/2018/06/22/605007387/supreme-court-rules-police-need-warrant-to-get-location-information-from-cell-to.

[10] Wessler, Nathan Freed. “The Supreme Court's Most Consequential Ruling for Privacy in the Digital Age, One Year In.” *American Civil Liberties Union*, 28 June 2019, www.aclu.org/blog/privacy-technology/location-tracking/supreme-courts-most-consequential-ruling-privacy-digital.

[11] “What Information Do VPN's Really Log?” *VPN University*, 15 Oct. 2015, www.vpnuniversity.com/learn/what-do-vpn-really-log.

[12] “What the Updated FISA Legislation Means for Your Privacy.” *Comparitech*, 21 Oct. 2020, www.comparitech.com/blog/vpn-privacy/updated-fisa-legislation-privacy/.

[13] “Your Data Is Shared and Sold...What's Being Done About It?” *Knowledge@Wharton*, 28 Oct. 2019, knowledge.wharton.upenn.edu/article/data-shared-sold-whats-done/.