**Policy Paper on Internet Privacy Protection**

Name

Institution

Date

**Policy Paper on Internet Privacy Protection**

**Introduction**

Technological advancement and the coming of age of the internet have provided many benefits for the present-day world. Individuals and organizations are reaping the benefit of having the internet easily accessible through numerous technological tools. These benefits include ease of communication and increased productivity within the government and businesses, as technology has made all activities faster than they were before their onset. Despite these advantages, there are numerous challenges the internet age has brought to the world. Privacy is on top of the list among these challenges. With the internet and various technological tools, more and more data is being generated faster, such that the organizations collecting this information cannot keep up. Cyber-criminals find this as an excellent opportunity for the exploitation of data which can wreak havoc in society. In the past decade alone, major U.S sectors have been affected by privacy issues in cases such as the Equifax breach, the snowball revelations, and even the Cambridge Analytica cases, among others. The issue of internet privacy is slowly becoming a losing game both for individuals and the legal system. This calls for immediate changes in the game's rules before society and the economy lose out in the end. Therefore, this policy paper explores internet privacy protection, analyzing the available policy options for solving this problem and later providing the best recommendations.

**Problem Statement**

In exploring internet privacy protection, it is first vital to understand the definition of internet privacy. This refers to the right/mandate of personal privacy individuals are entitled to upon storage of information on the internet. It is primarily concerned with how personal information can be exposed on the web through data collection, sharing, and other cybersecurity threats. In the modern technologically advanced world, digital footprints are found anywhere from giving an email address, filling out an online form, using a debit card, among other online activities. The release of personal information into cyberspace then brings in the all-important question of the people who will have access to that information. Even when there are information security programs in the organization where one submits their data, they are never 100 percent guaranteed, and if exploited, personal information can leak to unexpected places. Some leakages have happened in the past decade. This showcases the severity of this issue, as mentioned in the introduction. It is important to analyze some of these cases to understand better the problem of internet privacy in the U.S, which necessitates policy interventions.

The Snowden revelations in 2013 took the country by storm. Snowden, a government contractor, leaked information about the U.S government surveillance activities through the National Security Agency. The information surveilled included Americans' online and phone communications. Despite the 'positive' anti-terrorism efforts that the government was attempting to use this surveillance, the public was still concerned. Snowden was able to access this private information and leak it to the public. This compromises the issue of data and internet privacy. The government's ability to spy on this personal information was also viewed by some quarters as an abuse of civil liberties and the privacy of its citizens sparking a wide debate up to date (Clark, 2016). The government was not the only affected party with this leak, but American companies also felt the heat. These were the companies whose names and logos showed up in Snowden news stories. The companies had to deal with the severe suspicions and the loss of trust in their ability to keep private their consumer information. Geiger (2018) notes that most Americans (56 percent) still believed in the aftermath of this event that the courts were not providing adequate limits for the collection of online information. This showed a great gap on the issue of internet privacy protection.

The Equifax breach in 2017 also exposed the personal information of about 147 million people. It again raised the question of the safety and privacy of data on the internet. The company settled the issue through a government settlement with the Federal Trade Commission. This is because the company was found guilty of breaking the laws that were in place. While it is commendable that there were laws in place, this breach illustrates that there are still many policy gaps given that the data breach still occurred, necessitating the development of more stringent policies to deal with the evolving issues of internet privacy protection (Moore, 2017).

Similarly, the Cambridge Analytica scandal obtained data improperly through a third-party app from 87 million Facebook profiles. The objective was to ensure that they successfully unleashed a psychological warfare weapon against Americans for the election of former president Donald Trump. The company obtained this private information again raises the question of how safe people's data is on the internet amid the government's policies to curb the abuse of data on internet spaces (Hinds et al., 2020).

Further, in 2015, a Pew Research Center study revealed that 74 percent of Americans think controlling personal information is very important. The same study also revealed that 86 percent of Americans had taken various steps to maintain their internet privacy, such as the deletion of cookies, email encryption, and the protection of IP addresses (Pew Research Center, 2015). This shows a wide recognition of the threat of cyber-attacks and the lack of stringent internet privacy protection laws. People will continually use the internet. However, the question remains on the government's efforts to introduce policies that would prevent a repeat of history in internet breaches that expose private information shared over the internet. The three cases above all present the same issue in different lenses showing that there is still room for improvement as the internet continues to be widely famed as one of the most useful tools for the 21st century.

**Current Policy Environment**

In the above section, there has been plenty of reference on the policies in place on internet privacy protection. The understanding of these policies helps in comprehending the current policy environment in the U.S. This then provides a basis by which recommendations emerge on how to make better policies. Notably, there are no single laws that regulate online and internet privacy. Instead, there is only a patchwork of federal and state laws that apply, and cases revolving around internet privacy protection use these laws for operation. One of the key laws used about internet privacy is the Federal Trade Commission Act (FTC) of 1914. This Act has broad jurisdiction over commercial entities, although it does not explicitly deal with internet privacy laws. It seeks to prevent unfair and deceptive practices among private entities (Raul, 2014). Commercial entities must comply with posted privacy policies on their websites and protect consumer data with this law. It is important to note that the law does not specify or regulate the information included in website privacy policies. However, it will hold the company liable if it does not adhere to what it has posted.

The other policy associated with internet privacy laws is the Electronic Communications Privacy Act (ECPA) of 1986. This law seeks to protect unauthorized interception, access, and the use of wire, oral and electronic communications. For instance, in the NSA acquiring private information, this would have been an applicable rule, although the NSA indicated that it was doing so to fight terrorism. There is also the Computer Fraud and Abuse Act (CFAA) of 1986. This law makes it illegal to access a computer without authorization or excess authorization to access and obtain information or transmit harmful items within a network. The Children's Online Privacy Protection Act (COPPA) of 1998 prevents parties from accessing and using the personal information of minors below the age of 13 without parental consent. It also prohibits these parties from collecting and disclosing such information. The parental consent required should be verifiable, and the websites should post online privacy policies while still ensuring that they create and maintain reasonable security measures. The Financial Services Modernization Act (GLBA) of 1999 regulates the collection, use, and disclosure of financial institutions' personal information collected and held. The financial institution should seek the consent of the consumers when revealing such information. These laws are at the federal level, and several states have adopted laws affecting online privacy. Some of the laws adopted by states include consumer protection statutes, information security laws, data breach notifications, among others, depending on the state.

**Objectives**

The current reports on major data breaches have increased the demand for more federal legislation to guarantee internet privacy protection for consumers and society. As evident from the current policy environment section, the existing privacy laws developed as a series of responses to specific concerns. That is how the United States ended up with a patchwork of federal and state laws building up for more than a century. As more data is being collected, there is the realization that this system cannot continue to work. It cannot keep pace with the explosion of digital information. As such, the first objective of the federal government on internet privacy-related laws should be to develop laws that take into account the agile nature of the internet. These laws will recognize that the internet will not remain the same for years to come due to continuous improvement and innovation. As such, the laws should have foresight on the potential challenges. The other objective is to advocate for laws that clearly define the authorization that different entities have when accessing the information on the internet. There is also the objective of increasing the awareness of the consumer on the uses of their data. The lack of specificity in current policies leads to cover-ups in the name of the law. This then keeps consumers in the dark about the uses of their private information. Lastly, there is the objective of governing the collection and the sale of personal information to private sector companies such as information resellers.

**Policy Options**

In providing the policy options, it is important to continually understand the changing nature of the digital world that leads to the policy options provided. The policy options outlined in this section are;

1. Continuing with the status quo
2. Moving towards more regulation of emerging technologies, online tracking through the development of a unified federal law.
3. Policies that redefine the expectations of privacy.

The policy option of continuing with the status quo would see the government fold its hands and indicate that this is the con side of having the internet. As much as this offer may be tempting to avoid putting in the work, it would be detrimental to the economy and society. As mentioned above, poor internet privacy laws have seen companies act recklessly with consumer information, allowing even third parties to access and resell the information (GAO, 2019). Maintaining the status quo would see the companies continue to get away with settlements even when they have endangered consumer data. Companies would become lax when it comes to implementing controls that may seek to protect consumer information, leading to an internet laden with chaos. This would be the least strategic option and would accelerate the growth of the cyber-crime space in the U.S and globally.

The second option is moving towards more regulation of emerging technologies. As the spectrum of technology and the widely available and accessible data continues to widen, there is more falling outside specific laws on the books. These include more of the data generated through widespread use, including; data from web searches, social media, e-commerce, and the different applications on the phone, among others. This reflects the agile nature of the technological world. For instance, new applications are coming up every day that require the internet for their effective functioning. These applications have not been accounted for when it comes to the current laws. This means that individuals who access that information can exploit it since the law will not directly knock on their doors.

Another example is the expected connectivity of various devices with everything from cars to homes to street furniture. This has not been accounted for in the currently available laws that seek to protect internet privacy. It shows that the changes are coming faster than the legislation and the regulatory rules adaptation capabilities erasing the sectoral boundaries defining the privacy laws. With this knowledge, the belief is that the best way forward to solve the gap is to develop a unified federal law that considers all upcoming internet-related issues to protect the consumer. The policy should specifically cover emerging technologies and give guidelines on how to handle internet-related privacy. The government can also curb this problem through the regulation of online tracking and advertising. Currently, industry associations are responsible for setting rules for their members. This leads to a cycle where the laws are not stringent and can abuse users' internet privacy. The government regulation of emerging technologies will help in averting this.

Lastly, there is the option of redefining the expectations of privacy. The issue of expectations of privacy has challenged ongoing conversations on internet privacy. There is so much data available, and it is going through so many hands, changing the nature of protected information. This brings in the issue of the ability to maintain the anonymity of any source of information. It is becoming increasingly easier to link the anonymous information to its source and even derive their specific characteristics and personal information. Few laws are addressing this new reality, given that every information one releases to the internet has a 99 percent chance of falling into the hands of a third party somewhere. This new reality has increasingly challenged the judgment about the expectations of privacy and the definition of the scope of privacy protection even within different legal jurisdictions.

The belief then is that the best way to solve this issue is to introduce a policy that will define policy expectations. This will bring to light and introduce clarity to both the information holders and the information givers (the consumers) on what they should expect and offer. Consequently, both parties can decide the level of information that they are willing to part with. Additionally, in preventing unfair or deceptive practices, the FTC does not investigate the companies that disclose what they do to avoid trouble. This approach can be used to cover up some of the biggest mishaps in internet-related data. As such, there should be regulatory standards and constant audits to determine whether all organizations comply or are engaging in any deceptive practices.

**Recommendation**

The policy recommendation that would suit the policy challenges revolving around internet privacy protection is regulation of emerging technologies and online tracking. This would be through developing a unified federal law that works in all states to regulate any emerging technology. Regulation of emerging technologies is quite important as it incentivizes the service providers to respect the privacy of internet users (Nyoni et al., 2020). The lack of regulations is mostly leading to new technology misuse, which is a violation of the users' privacy. The main reason this is the recommended policy is that it provides an all-encompassing approach and solution to the problems of internet privacy protection. The unified federal law will be quite impactful as the U.S constitution clearly states that whenever a state law has a conflict with the federal law, then the federal law will be the one put in use. This means that the state laws with general applicability will have the unified federal law regulating the emerging technologies to follow and specify unclear policies. The unified law will also have a preemption provision aimed at the directly conflicting state laws.

Regulation of emerging technologies will help address different privacy risks mentioned as challenges in the current policy environment revolving around the issue. Privacy breaches are viewed among the common and most fatal risks to privacy. This has led most internet users to view their data as important and strive to find strategies to reduce the likelihood of this risk. The other risk is that of hackers who are mostly responsible for the privacy breaches. Hackers can execute their cybercrimes that lead to breaches even though the theft of data from individual users.

Further, the Internet of Things (IoT) has brought many devices that are useful in day-to-day activities. These can be a threat to privacy as every manufacturer has a diverse set of products. This diversity and uniqueness of the products make compatibility difficult and affect the design of secure IoT. All the above are examples of emerging technologies which this policy would help reduce the accompanying risks. Hackers will look to the emerging technologies before the developers attempt to understand any vulnerabilities and block the same. As such, the regulation of these technologies will ensure that they come up when minimal vulnerabilities are reducing the risk of having privacy breaches.

Opponents of this regulation may argue that this will impede innovation due to the long regulatory requirements and monitoring. However, these long processes are better to protect the consumers and society in general. The alternative would be dealing with the aftermath of internet privacy breaches. These have wreaked havoc in the United States in the past. Further, there may also be the argument that public data privacy can be achieved through the anonymization of information. This is not a guarantee or likelihood in the present day. Emerging technologies have made it easy to identify individuals from anonymized sets of data which presents a challenge of data privacy that can be solved by regulating emerging technologies (Stankovic, 2019).

**Conclusion**

Undoubtingly, a privacy legislation in America is integral due to the numerous changes occurring in the digital world. There have already been numerous threats orchestrated in American cyberspace that threaten society's trust in the government's ability to provide internet privacy. The gaps identified involve the lack of clarity in the available policies as they are not updated. This prevents tackling problems as they emerge. Consumers and citizens, in general, need to trust that data about them will be used, stored, and shared in responsible ways. Building high levels of trust is an essential building block to having a strong digital world since the U.S is a global leader. The policies adopted in the country will greatly influence how other countries will view their internet privacy-related laws. The recommended regulation policy will greatly contribute to trust-building, which enables data-driven knowledge and innovation while laying out guard rails for the protection of privacy.

**References**

Cameron, Kerry, John, Morris, Caitlin, T., & Turner Lee. (2020). *Bridging the Gaps: A path Forward to Federal Privacy Legislation.* Retrieved from <https://www.brookings.edu/wp-content/uploads/2020/06/Bridging-the-gaps_a-path-forward-to-federal-privacy-legislation.pdf>

Clark, I. (2016). The digital divide in the Post-Snowden era. *Journal of Radical Librarianship*

Geiger, A. (2018). *How Americans have viewed government surveillance and privacy since Snowden leaks.* Pew Research Center

Government Accountability Office (GAO) (2019). *Consumer Privacy: Changes to Legal Framework Needed to Address Gaps.* Retrieved from <https://www.gao.gov/products/gao-19-621t>

Hinds, J., Williams, E., & Joinson, Adam. (2020). “It wouldn't happen to me”: Privacy concerns and perspectives following the Cambridge Analytica scandal. *International Journal of Human-Computer Studies*. 143

Moore, Tyler. (2017). On the harms arising from the Equifax data breach of 2017. *International Journal of Critical Infrastructure Protection.*

Nyoni, P., Velempini, M., & Mavetera, Nehemiah. (2020). Emerging Internet Technologies and the Regulation of User Privacy. *The African Journal of Information Systems*

Pew Research Center. (2015). *Americans’ Views About Data Collection and Security.* Retrieved from <https://www.pewresearch.org/internet/2015/05/20/americans-views-about-data-collection-and-security/>

Raul, A. (2014). *The Privacy, Data Protection and Cybersecurity Law Review.* Retrieved from <https://www.sidley.com/-/media/files/publications/2014/11/the-privacy-data-protection-and-cybersecurity-la__/files/united-states/fileattachment/united-states.pdf>

Stankovic, M. (2019). Regulating Emerging Technologies: Opportunities and Challenges for Latin America. *Proceedings of Science*