Petition to Enact Comprehensive Privacy Laws in New Jersey

To safeguard the privacy rights of New Jersey residents and ensure their ability to exercise control over their personal data, including options to **access, modify, delete, or opt out of the sale of such data to third parties.**

Abstract

This petition calls for the enactment of comprehensive privacy laws in the state of New Jersey. As technology progresses at a rapid pace and more personal data is collected and shared online, existing laws have not kept up with protecting the fundamental privacy rights of citizens. Comprehensive privacy legislation has already been successfully established in other states and nations to safeguard individual rights. This petition argues that residents of New Jersey deserve strong legal safeguards and transparency regarding how their personal information is collected, used, and shared by both companies and the government. The proposed laws would establish clear rights for individuals to access, modify, delete or opt out of the sale of their data to third parties. Such legislation has been shown to increase consumer awareness of data privacy practices and encourage companies to raise capital through business models that respect individual consent. The case will be made that enacting privacy laws is crucial to upholding privacy as a basic civil liberty in the digital age.

Rationale and Justification

Personal data is collected, sold, and used daily by almost all internet-connected companies, often without the knowledge or consent of the consumer utilizing their services. Projects such as Spyware Watchdog (https://spyware.neocities.org) and ToS;DR: Terms of Service; Didn't Read (https://tosdr.org) have sprouted up to combat the obfuscation of how data is mined and to inform users about what actually happens with their data.

For example, the service Reddit decredits your content and "you irrevocably waive any claims and assertions of moral rights or attribution with respect to Your Content." (Reddit, 2023). Spyware Watchdog, the service mentioned above, has collected evidence from various sources that Google Chrome keylogger, constantly records active microphone channels, profiles your device usage, and sends your passwords to their servers. In addition, they create a unique identifier per install, "so that Google can create a consistent user identity for you, undermining anonymity." (Spyware Watchdog, 2021).

These examples are completely non exhaustive. A quick google search leading to the privacy policies of various companies can give you quick insight onto how data is handled, provided it is thoroughly analyzed. For example, the TikTok privacy policy collects your usage, device, location data, device information, cookies, and more by your usage of the service. However, they also collect information from "Advertisers, measurement and other partners" which include your activity on other platforms, and "such as mobile identifiers for advertising, hashed email addresses and phone numbers, and cookie identifiers, which we use to help match you and your actions outside of the Platform with your TikTok account." (TikTok, 2023).

Similarly, the blue chip Microsoft, which created the illusion of a transparent operating system Windows, is known for being a notorious privacy nightmare. Let's dive into some of the ways Windows collects your data. When monitored under WireShark (https://www.wireshark.org/), a free utility to monitor network traffic in real time, the company requested the usual Bing, Windows Update or SmartScreen, and in addition third party geolocation servers and those which belong to largely unknown entities, on idle. In total, Windows "had tried over 5,500 connections to 93 different IP addresses, out of which almost 4,000 were made to 51 different IP addresses belonging to Microsoft." In these 5,500 requests are contained a variety of data regarding voice, hardware, internet, browsing history, application logs, and more (TheHackerNews, 2016).

Finally, it is worthwhile to mention Apple, which is regarded as a privacy-friendly company. With your "consent", Apple collects hardware, contact, payment/transaction, health, fitness, financial information, and your application usage data. They also collect information passively from their partners, which includes data from other individuals when they "[have] sent you a product or gift card, invited you to participate in an Apple service or forum, or shared content with you." They also send data to third parties to "validate the information you provide" (Apple, 2022). In comparison to the above examples, Apple does protect the privacy of their users more effectively, but they still collect a vast amount of information about their users.

Another major concern is security breaches. Since no company is able to provide perfectly secure software, therefore larger amounts of data means a larger attack surface. If the companies software gets breached, mass amounts of personal data, potentially for hundreds of thousands of users- are now accessible to a group with malicious intentions. As companies tend to store passwords in plain text on their servers, this could be utilized to compromise data on a variety of other servers, as well. Not even the federal government is completely insured against attacks, as notable in the 2020 federal government breach by Russian hackers on the company SolarWinds which is a product employed to monitor network activity on federal systems. This lead to "nearly 18,000 of its customers [receiving] a compromised software update" (GAO, 2021).

Not all hackers are experienced, some are still in secondary school! Earlier this year, teenager hackers loosely banded from places like the UK and Brazil exploited security weaknesses in major businesses in the United States. If even teenage hackers could penetrate systems of such large corporations, then what is to be said about the more experienced hackers? Even if the access point to this breach was completely patched, "it could take a decade eradicate a vulnerability in software used by thousands of corporations and government agencies worldwide." (Lyngaas, 2023).

It is important to consider that New Jersey does have standard measures for a company to take in the event of a data breach, which includes "notification of the breach to any customer who is a resident of New Jersey whose personal information was, or is reasonably believed to have been, accessed by an unauthorized person." (Disclosure of Breach of Security to Customers, 2023). However, this does not grant the consumer the ability to exercise rights over their data, and additionally the consumer cannot prevent leakage of their personal data nor reduce the effects.

Unfortunately, companies have it difficult to market to the consumer, than in the past. Businesses release almost 30,000 products every year, "and 95% of them fail according to Clayton Christensen, a

professor at Harvard Business School." (Geraldo, 2021). For this reason, many companies data mine their audience in an attempt to build more relevant ads for the consumer. It is important for companies to understand that data mining is not a standard policy to be adopted for their marketing model, and that innovative measures should be taken for a more moral model of reaching their consumers.

Additionally, the demand for smartphones have increased steadily in recent years, and contain several telemetry features, such as precise location data, detailed video/microphone input, and very accurate logs of how the user interacts with the device. Not only smartphones, but smart watches, such as the Apple Watch, which tracks your heart rate, blood pressure, body temperature, and can even gain some insight into your emotions; which companies that track the music its consumers listens to, like Spotify, already have perfected on higher levels.

It is important to understand that while these services may track you and profit significantly off of your personal data, even if they were completely privacy friendly, there are flaws in the services that these companies may make. For example, the content of iMessage conversations "are encrypted end-to-end, so they can't be read while they're sent between devices." (Apple, 2019). However, Apple's services use iCloud, and iCloud backs up contents of the iPhone including messages to their servers, where it is stored in text format regardless. Apple may address this in the future.

While a significant amount of information was provided regarding how companies are not transparent or cooperative with personal data, this is not to say that these services do not have their uses. In the increasingly digital world, where even realities are simulated, these applications have provided convenience. Smartphones have integrated a variety of features that would require an array of devices in the past into one, such as documents, music, camera, texting/calling, emails, and more.

Smartwatches have made it significantly easier to be able to monitor one's physical statistics, as well as provided convenience to notifications on their smartphones which would require turning on the smartphone and unlocking it before being able to view information on the notification. Spotify and other music products like Apple Music have made organization of music a bliss, and being able to listen to each other's collection of music a simple and easy process as well. They have also opted for protection of their creators content utilizing a proprietary technology known as DRM or Digital Rights Management, which allow secure playback of the content. Utilizing school or university services almost always requires an online account. To navigate the modern world without creating an account on any internet services would be a very difficult, if not impossible task.

These proprietary, commercial technologies that often come with an illusion that they carry no price, profit massively from mining personal data. This has been in due to the internet being portrayed as a large, free entity, on which nothing should have a price, following it's exponential increase in the late 90s. In some way, this statement is correct, but to those who can spare a few measly dollars, the cost of surveillance is much higher. Companies have done a rather exceptional job of portraying the value of the service as a mere representation of the price that you pay, allowing them to degrade their service to sweetened garbage without having to base their reasoning for doing so on a less valid excuse.

That's not to say that proprietary technologies don't charge you, either. For example, services may allow automated sign up and subscription payment online, but require calls and a wait in line to cancel. For many users, the monthly subscription payment consumes a portion of their bills without their

knowledge, a process referred to as automatic bill payment. If the user had a streamlined process to delete their account after the necessity of the service terminates, then the subscription payments would be canceled as the account would cease to exist.

It should be mentioned that privacy respecting software, commonly open source software, have the potential to being a viable alternative. It is possible for one to switch the majority of their software to the privacy respecting alternatives without having to worry about the quality of the software; however, migrating existing infrastructure already causes huge discrepancies, and for needs such as educational or financial to be met, software with tracking features are usually the only option. Therefore, it is more viable to be able to modify, access, and opt out of the sale of the users data while the software is being utilized, and for the data to be discarded once the purpose has been succeeded.

If New Jersey is able to adopt a law that would grant users rights to modify, access, delete, or opt out of the sale of their data, numerous things would happen. Firstly, the profitability of mining users data would decrease with publicity. Citizens will contain a greater understanding of how corporations may use and control their data, motivating them to read privacy policies in the future, and to keep track of services in which the citizen is enrolled in. Corporations will receive that New Jersey is granting rights of control over its citizens data and this may motivate other states/countries to do so. Data deletion/opt out of sale/access requests incur a small cost to the organization, and with increasing education about privacy, it could become less profitable overall, requiring companies to adopt a more moral, innovative method of profiting off of their products. It would inevitably lead to improved marketing and higher standards of quality for their products, due to increasing awareness of other immoral actions companies may commit, such as relying on poor labor conditions in developing countries for the low prices we see today.

Even though commercial products may be notorious for monetization in whatever means possible, they are not all negative. If innovation is channeled properly, more moral, healthier, environmental friendlier business strategies will spring about. Passing the New Jersey Privacy Act is the start to an improved world where businesses have other, more moral and transparent methods of profitability.

Also, a significant of internet services do provide account deletion as a feature of their website, whether there is a legal requirement for it or not. Notably, the majority of the organizations mentioned throughout this document, do allow the user to delete their account through the website. TikTok (https://tiktok.com), Instagram (https://instagram.com), Reddit (https://reddit.com), Google (https://google.com), Microsoft (https://microsoft.com), Spotify (https://spotify.com), Discord (https://discord.com), and many more provide the ability to delete data right from the website.

However, there are notable services that require manual contact and a tedious verification process to delete one's account. For example, services may allow automated sign up and subscription payment online, but require calls and a wait in line to cancel. Macy's (https://macys.com, Zillow (https://zillow.com), NinjaKiwi (https://ninjakiwi.com), Steam (https://store.steampowered.com), Supercell (https://supercell.com), and other organizations require email or phone contact. In addition, organizations like Teespring (https://teespring.com), Peacock TV (https://peacock.tv), NewEgg (https://newegg.com), and Amazon AWS (https://aws.amazon.com) are stringent on their data deletion policy, and may take notorious periods of time to comply with the request, and may refuse to comply

where privacy rights are not mandated by law. One of the most notorious organizations, Roblox (https://roblox.com), require manual verification that the consumer is in a jurisdiction where legal rights can be executed requiring use of your camera and mic and related technologies in order to for them to comply with the request.

Therefore, one could argue that even with the privacy laws, things may remain imperfect. Even for companies operating in jurisdictions that require enhanced privacy laws, the user is often asked the question several times if they would like to delete their account in “confirmation” and have a scheduled deletion time of a few months. Additionally, the process may be manual and the customer service may be largely unresponsive. There may still be difficulty in exercising privacy rights regarding your personal data due to the companies unyielding nature, however the process of exercising privacy rights will become much easier due to the necessity to comply with law. When equipped with a legal requirement, like 45 days as established in other states, it becomes much more likely that the companies will comply with your request, and if not you have the legal authority to file a complaint on NJ Consumer Affairs (https://njconsumeraffairs.gov) against them at your discretion, which has the added bonus of reducing the companies popularity and decreasing the likelihood of other companies refusing to comply. The purpose of the law is not for perfection, but to grant consumers in New Jersey easier access to exercising privacy rights, and to inform the general public about how active action is being taken against data mining.

However, New Jersey would not be the first state to adopt privacy laws, either. Numerous acts have been enacted in legislatures across the United States and in other regions to empower consumers to regain control of their data. Examples include the Colorado Privacy Act (Colorado General Assembly, 2022), California Consumer Privacy Act (State of California Department of Justice, 2023), Connecticut Data Privacy Act (Connecticut State, 2022), and the Virginia Consumer Data Protection Act (Code of Virginia, 2023). All of these acts allow consumers to modify, access, delete, and opt out of the sale of their data. They were enacted out of a growing concern about data collection in their states.

Neither is the United States the first nation to adopt laws regarding data rights. These rights have been adopted in laws such as the Act on Protection of Personal Information (Japan, 2003), the General Data Protection Regulation (European Union, 2016), Data Protection Act (UK, 2018), Canada’s Personal Information Protection and Electronic Documents Act (Branch, 2019), Brazil’s General Data Protection Law (Brazil, 2018). It is important for the United States to be progressive with its data regulation policies as well. The New Jersey Privacy Act will be a predecessor to that.

As a state, New Jersey grants the consumer a significant amount of rights. New Jersey has passed acts such as the New Jersey Consumer Fraud Act (New Jersey, 2022) which protects consumers from fraud and allows individuals to seek damages for losses suffered, Truth-in-Consumer Contract, Warranty, and Notice Act (New Jersey, 1981) which ensures clear and accurate information in businesses contracts, warranties, and notices and prohibits unfair and deceptive provisions, Lemon Law which protect New Jersey consumers who “purchase vehicles that develop repeat defects or lengthy unusable periods during the first two years or 24,000 miles.” (New Jersey, 1989), and the Identity Theft Protection Act, which sets requirements for businesses to secure personal information and to notify the consumer of “any breach of security of those computerized records following discovery or notification of the breach to any customer who is a resident of New Jersey whose personal information was, or is reasonably

believed to have been, accessed by an unauthorized person." (New Jersey, 2020). Moving into a more digital age, is it not colossal that New Jersey doesn't have basic data protection laws for its citizens?

In addition to the New Jersey laws stated above, it is important to note that there are existing federal privacy laws, such as the Children's Online Privacy Protection Act which "imposes certain requirements on operators of websites or online services directed to children under 13 years of age, and on operators of other websites or online services that have actual knowledge that they are collecting personal information online from a child under 13 years of age." (Federal Trade Commission, 2013), and the Gramm-Leach-Bliley Act (Congress, 2000) which protects financial information. However, these federal laws do not provide sufficient protection and are very specific, as opposed to a general protection law that encompasses the majority of corporations. New Jersey residents still lack control over their personal data in the vast majority of cases, allowing companies to harvest and sell it to third parties at their discretion. The New Jersey Legislature has considered enacting privacy rights in the Disclosure and Accountability Transparency Act (Gopal, 2023). Why should the ability to exercise privacy rights of New Jersey residents continue to suffer?

By signing this petition, you commit to the belief that citizens should have the right to control their personal data and should be able to access, modify, delete, or opt out of the sale of their data as desired. Help us make the New Jersey Privacy Act a reality and strengthen residents' privacy rights.

References

Home - Spyware Watchdog. (n.d.). Spyware.neocities.org. Retrieved December 3, 2023, from https://spyware.neocities.org

Team, T. (2019). *Terms of Service; Didn't Read*. Tosdr.org; Terms of Service; Didn't Read. https://tosdr.org

User Agreement - September 25, 2023 - Reddit. (n.d.). Www.redditinc.com. https://www.redditinc.com/policies/user-agreement-september-25-2023

Google Chrome — Spyware Watchdog. (n.d.). Spyware.neocities.org. Retrieved December 3, 2023, from https://spyware.neocities.org/articles/chrome

TikTok. (2023, May 22). *Privacy Policy | TikTok*. Www.tiktok.com. https://www.tiktok.com/legal/page/us/privacy-policy/en

Wireshark Foundation. (2016). *Wireshark*. Wireshark.org. https://www.wireshark.org/

Windows 10 Sends Your Data 5500 Times Every Day Even After Tweaking Privacy Settings. (n.d.). The Hacker News. Retrieved December 3, 2023, from https://thehackernews.com/2016/02/microsoft-windows10-privacy.html

Apple. (2022). *Legal - Privacy Policy - Apple*. Apple Legal.

https://www.apple.com/legal/privacy/en-ww/

U.S. Government Accountability Office. (2021, April 22). *SolarWinds Cyberattack Demands Significant Federal and Private-Sector Response (infographic)*. Www.gao.gov. https://www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic

Lyngaas, S. (2023, August 10). *Homeland Security report details how teen hackers exploited security weaknesses in some of the world's biggest companies | CNN Politics*. CNN. https://edition.cnn.com/2023/08/10/politics/dhs-hacking-report/index.html

56:8-163 Disclosure of breach of security to customers. (n.d.). Lis.njleg.state.nj.us. https://lis.njleg.state.nj.us/nxt/gateway.dll/statutes/1/53120/53504

Diego.Geraldo. (2021, December 13). *Product Innovation: 95% of new products miss the mark | MIT Professional Education*. MIT Professional Education. https://professionalprograms.mit.edu/blog/design/why-95-of-new-products-miss-the-mark-and-how-yours-can-avoid-the-same-fate/

Apple. (2019). *Privacy - Features*. Apple. https://www.apple.com/privacy/features/

Protect Personal Data Privacy | Colorado General Assembly. (n.d.). Leg.colorado.gov. https://leg.colorado.gov/bills/sb21-190

State of California Department of Justice. (2023, May 10). *California Consumer Privacy Act (CCPA)*. State of California - Department of Justice - Office of the Attorney General. https://oag.ca.gov/privacy/ccpa

The Connecticut Data Privacy Act. (n.d.). CT.gov - Connecticut's Official State Website. https://portal.ct.gov/AG/Sections/Privacy/The-Connecticut-Data-Privacy-Act

Code of Virginia Code - Chapter 53. Consumer Data Protection Act. (2023). Virginia.gov. https://law.lis.virginia.gov/vacode/title59.1/chapter53/

個人情報の保護に関する法律 | e-Gov 法令検索. (n.d.). Elaws.e-Gov.go.jp. https://elaws.e-gov.go.jp/document?lawid=415AC0000000057

GDPR. (2018). *General Data Protection Regulation (GDPR)*. General Data Protection Regulation (GDPR); Intersoft Consulting. https://gdpr-info.eu/

UK Government. (2018). *Data Protection Act 2018*. Legislation.gov.uk. https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

Branch, L. S. (2019, June 21). *Consolidated federal laws of canada, Personal Information Protection and Electronic Documents Act*. Laws-Lois.justice.gc.ca. https://laws-lois.justice.gc.ca/ENG/ACTS/P-8.6/page-1.html

L13709compilado. (n.d.). Www.planalto.gov.br. http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm

Consumer Fraud Act. (n.d.). Retrieved December 17, 2023, from https://www.njconsumeraffairs.gov/statutes/consumer-fraud-act.pdf

TRUTH-IN-CONSUMER CONTRACT, WARRANTY AND NOTICE ACT. (n.d.). Retrieved December 17, 2023, from http://www.civiljusticenj.org/wp-content/uploads/2016/10/16Fall_TCCWNA_N.J.S.A.56.12-14-18.pdf

NJ MVC | Lemon Law. (n.d.). Www.nj.gov. Retrieved December 17, 2023, from https://www.nj.gov/mvc/vehicletopics/lemonlaw.htm

Identity Theft Protection Act . (n.d.). https://www.njconsumeraffairs.gov/Statutes/Identity-Theft-Prevention-Act.pdf

Federal Trade Commission. (2013, July 25). *Children's Online Privacy Protection Rule ("COPPA")*. Federal Trade Commission. https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa

GRAMM-LEACH-BLILEY ACT. (2000).

https://www.govinfo.gov/content/pkg/PLAW-106publ102/pdf/PLAW-106publ102.pdf

STATE OF NEW JERSEY 220th LEGISLATURE Sponsored by: Senator VIN GOPAL District 11 (Monmouth) SYNOPSIS "New Jersey Disclosure and Accountability Transparency Act (NJ DaTA)"; establishes certain requirements for disclosure and processing of personally identifiable information; establishes Office of Data Protection and Responsible Use in Division of Consumer Affairs. CURRENT VERSION OF TEXT As introduced. (2023). https://pub.njleg.state.nj.us/Bills/2022/S4000/3714_I1.PDF

To sign this petition, please provide your full name, city of residence, contact information, and signature to demonstrate your support for stronger privacy protection for New Jersey residents. Your information will not be disclosed without your explicit consent.

Please note that the structure and the information given in the petition may be subject to change. The purpose of this petition will remain constant.

Full Name	City of Residence	Contact (Email/Number)	Signature