ILLUMINATING THE DIGITAL LANDSCAPE: DISTILLING DIGITAL DATA PRIVACY AND ONLINE IDENTITY

By

Alex Dabecki

BA, University of British Columbia, 2020

A CRITICAL AND PROCESS DOCUMENTATION THESIS PAPER SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF

MASTER OF DESIGN

EMILY CARR UNIVERSITY OF ART + DESIGN

2024

Abstract: This thesis examines the commodification of user data by corporations like Facebook and Google. It proposes a user-centric approach to online privacy through a prototype application that visualizes and empowers users to manage their data footprint. The research assesses the effectiveness of Virtual Private Networks (VPNs) and argues that browser extensions and HTTPS browsing offer sufficient protection for most users. Furthermore, it explores methods for fragmenting digital identity, analyzing anonymous email forwarding services and password-less login protocols. While acknowledging the comprehensive privacy suite offered by Apple, the thesis cautions against vendor lock-in. An analysis of privacy solutions reveals limitations in both VPNs and App Tracking Transparency (ATT) initiatives. This emphasizes the need for stricter data practices and user control mechanisms within app ecosystems. The thesis recognizes the importance of user education, but highlights the limitations imposed by complex legal frameworks and a lack of stringent data privacy laws in the United States. It emphasizes the crucial role of individual knowledge in safeguarding personal data. The research concludes by reframing online privacy as the user's right to control, rather than anonymize, their digital identity and data. It underscores the importance of data literacy and informed decision-making regarding privacy settings. Ultimately, the thesis advocates for a balanced approach that empowers users to navigate the online world with both security and convenience, fostering a sense of data ownership over mere anonymity.

Keywords: data commodification; digital identity fragmentation; online privacy vs. anonymity; informed user choice; data ownership; VPN efficacy; internet privacy

Table Of Contents

The New Kid On The Block

A change is occurring in our global economy, but one that we arguably cannot see nor understand. Right in front of our eyes, transactions are happening with every tap and click yet remain completely invisible. Our activity is becoming more valuable but in ways that are difficult to understand because of the novelty of its use. Redundant to you and me, but liquid gold to others. What is the value, anyway? The European Union's position on data privacy is one of the strictest and most comprehensive in the world. It prioritizes individual rights and aims to create a fair and transparent environment for data processing. It sounds serious. A similar framework is yet to exist in the United States, home to many social media companies used around the globe. I want to explore why this is the case, and what tools consumers have at their disposal to protect their own self in situations without government regulation or for more robust privacy options. Why is what we do so valuable to certain people, what gives it value and how much is it worth?

Throughout my research I focus on an Apple-biased ecosystem used by everyday consumers. I do this for two reasons: I primarily use Apple products in my everyday life, and I have familiarity with system settings and capabilities of what I can (and cannot) do within the system. I also chose to focus on Apple because that is primarily what I see around me. Due to my insistence on exploring how privacy and security intertwine with everyday consumers, what I see every day is predominantly Apple products. As I acknowledge that Apple has limitations, the tools and solutions I delve into have good interoperability between operating systems and workflows that could be implemented in other ecosystems with minor modifications.

If The Product Is Free, You Are The Product

Discussing how physical beings produce digital data is important to dissect as this action is often invisible yet has profound impact on our lives. Illuminating these transactions that occur in the shadows is crucial to understand how little is known about the resource known as data. In the past, capitalism relied on the exploitation of labor and natural resources but has now shifted to the exploitation of personal data. “It is obscene to suppose that this harm can be reduced to the obvious fact that users receive no fee for the raw material they supply” (2019, p. 94) states Shoshana Zuboff, a social psychologist and author exploring the societal impacts of data collection and surveillance. She claims that the initiation of surveillance capitalism started from Google and Facebook, harvesting very large amounts of data from its users to then make a profit. In his book Data and Goliath, Bruce Schneier walked a similar path years before Zuboff. When data collection first started becoming prominent, storing data was too expensive. Metadata (data of data) was often thrown away. Now, it’s easier and cheaper to save and search rather than sort and delete - All data is stored (Schneier, 2016). Companies like Facebook and Google became the new Getty’s, but the commodity is not finite like oil – it is infinite.

A recent example of the value of user data was the mobile game Pokémon Go, developed by Niantic Labs and had 232 million active users at its peak in 2016 (Orvill, 2024). The game operated as a scavenger hunt for users to collect Pokémon in the real world using augmented reality and the user’s GPS coordinates. It was lauded for promoting physical activity and pioneering new game styles since users had to physically visit “PókeStops” through AR technology. It is interesting to note that Niantic Labs was born as an internal start-up within Google five years prior to Pokémon Go’s announcement. Niantic says they are “a gaming company with an outsized passion for getting gamers outside” (Mehrotra & D’Anastasio, 2019), a great mission statement to get people out and about. However, this passion sparked controversy during initial launch, which

involved users giving Niantic a huge number of permissions: contacts, location, storage, and camera. iPhone users also turned over full Google account access, which was not integral to gameplay. Metadata is just as valuable as data, especially when algorithms are in place to piece everything together into who you are and what you do, where you go and when you do.

A notable event that took place in 2018 involving Facebook known as the "Cambridge Analytica data scandal" was a catastrophic misuse of user data that Facebook did not take accountability for, and no improvements were seen by the users as a result (Confessore, 2018). 87 million profiles were harvested for the purpose of political advertising, specifically for the presidential campaigns of Donald Trump and Ted Cruz (Meredith, 2018). While the users accept the terms and conditions and company privacy policies when registering for an account, the Cambridge Analytica scandal highlights the sheer amount of data a user is producing that has value for the company.

Data As A Commodity

As part of my early research, I wanted to explore how data is viewed from more of an overview from the device itself. Building a quick prototype to see how it would look, it evolved into a *Data Wallet*. I was inspired by Apple's own Wallet app, but instead of showing financial transactions, it would show data transactions. I used information from Apple's App Store to find data points certain apps used to track their users, and built them into more readable "cards", replacing credit card details with application details instead. The aim of this was to highlight how much data an app used and what category it fell under – Contact Info or Location, for example. As it was early in the research, I asked fellow classmates what they thought about it. Some common threads were that it was an interesting idea to visualize data in such a way, but the implementation might prove to be more cumbersome than originally predicted. As l learned much later, these data points were not reliable. I expand this more in a later section When Privacy Falls Short.

Figure 1: First iteration of Data Wallet. Inspired by Apple's Privacy Labels from the App Store.

I wanted to expand Data Wallet into a more purposeful application that gave users power to control what data left their device. This had major caveats, as it assumed that the application owner will agree to sell a user's data only if they request to do so. A large ask, even for policy juggernauts like the European Union. I also wanted to add a value proposition to a user's data, meaning I wanted a financial incentive for a user to explicitly see their data as a dollar value and have the power to choose what to do with that. This shift was inspired by a project I worked on in my first semester at Emily Carr, looking at an online shopping experience from the perspective of web trackers. In front of

Figure 2: Ability to View Accessed Data.

fellow classmates, I decided to walkthrough a simple laptop purchase starting from Google and ending at the checkout of Lenovo. This took approximately three minutes and resulted in 171 trackers, a significant portion coming from Facebook and Google. The reason I wanted to demo this to the class is to highlight the impact we have on companies and how our browsing habits have inherent value we may be unaware of. Facebook, a major player in the cookie tracking space, made $116.6 billion USD in 2022 (Meta, 2023). It begs the question – what do they sell?

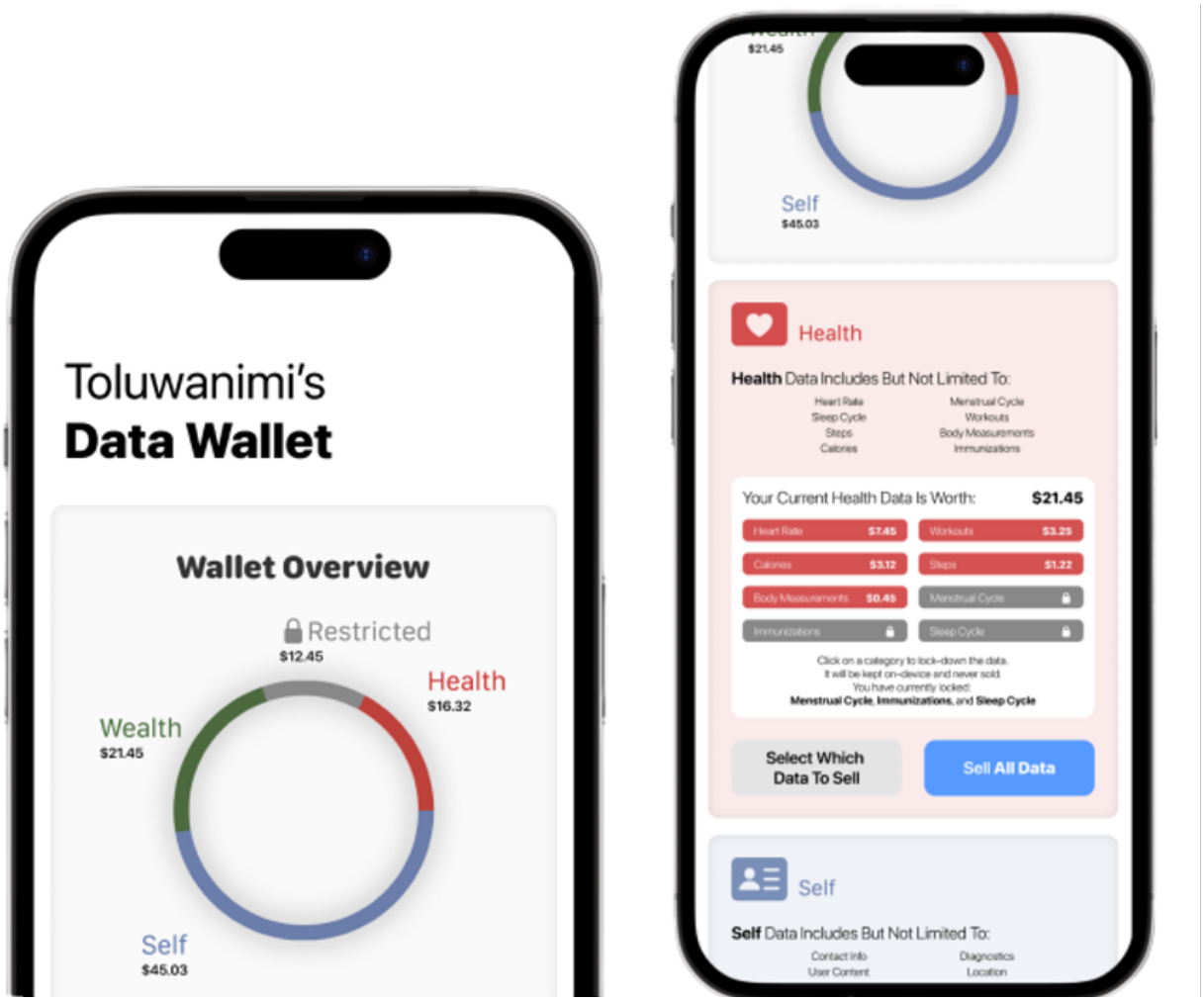

Figure 3: Second iteration of Data Wallet, moving away from App Data and towards User Data and the perception of Data Value.

Creating the second version of Data Wallet meant finding a way to connect some form of value to a user's data. It was challenging to get realistic values, so all figures represented are simply for demonstration purposes only. Assigning value to different categories allowed the user to decide what was worth selling and what was worth keeping private. Data Wallet also allowed different tiers of anonymity that reduced amount of linked information to the sold data, in exchange for less face value. The goal was to add a sense of user interaction; rather than simply viewing data leaving the device, the user can act upon it.

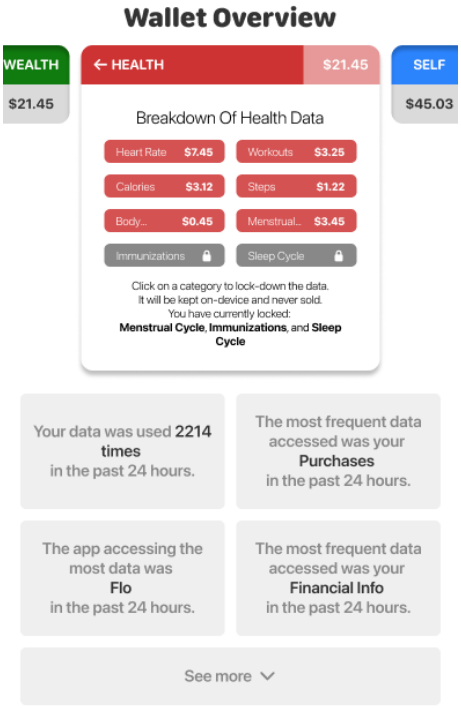

Figure 4: Detailed View of Data Wallet V3

A final version of Data Wallet was created to combine elements from both versions, as they had something unique to contribute to the visualization of user data. Adding the application cards to the bottom of the screen and combining the value proposition of selling user data. I didn't pursue this further as it was merely for exploration purposes, and upon further discovery (as mentioned prior) inaccurate. Figure 4: Detailed View of Data Wallet V3 shows how both features of the prior Data Wallet combine into one seamless experience in V3.0, viewing the value of their data along with how the data is accumulated and from which source(s).

Tools of Privacy

Multiple tools exist for the purpose of privacy and data protection. They can be as simple as an action or as rigorous as a dedicated piece of equipment. Understanding the spectrum of tools was interesting to discover because of the different nuances between them, benefiting some but potentially not others. Exploring how such tools could be implemented into everyday workflows is important for this research, as strategy can only go so far without the necessary tools. Software such as a Virtual Private Network (VPN) is a common example of a security tool used by many user groups, from office workers accessing company information to suppressed citizens requiring blacklisted websites or media. There are other tools available, such as a change in browsing habits, that I will discuss later as they are on a different part of the security spectrum with their own benefits and downsides.

Virtual Private Networks

During my investigation, I was exposed to a plethora of advertisements for various Virtual Private Network (VPN) clients, each promising attractive deals and multi-device support at comparable prices. My preconceptions about these VPNs were largely influenced by Sun Knudsen, an independent privacy and security researcher known for his comprehensive "privacy guides" on various platforms and products. I found it important to discuss VPNs as part of my research because they were frequently mentioned in privacy-related discussions and had great marketability when it came to advertisements. However, the nature of VPNs became a double ended sword. They did indeed provide privacy and security to its users, but I wanted to explore if the inverse was also correct – were VPNs the right solution for users that wanted to increase privacy and security in their digital life. My objective was to strike a balance between utility and genuine privacy protection. The VPNs I evaluated had diverse pricing structures, with most offering a free trial period and others charging a flat monthly rate. It needs to be stated that the use of a VPN for these tests is simply for privacy protections, not

for accessing geo-locked content nor workplace computers. The conclusions are based simply on the fact of delivering a good experience with strong privacy which may include internet speed, secondary features/perks, and integration into daily use.

A Virtual Private Network (VPN) operates by directing all internet traffic through a secure tunnel, which is then relayed to one or more servers, typically managed by the VPN provider, before reaching the intended IP address. The availability of numerous servers for relaying enhances the speed of traffic flow. A significant concern for all VPN providers is a breach in the secure tunnel, an incident that occurred with a prominent VPN (Williams, 2021). Such a breach is alarming because, if compromised, the secure tunnel's entry and exit points, representing your IP location and target IP location, become exposed. Depending on the severity of the attack, the implications may extend further. Mullvad, for instance, mitigated this situation by eliminating any links to potential financial or personal identification within the product.

Surfshark

I commenced my evaluation with Surfshark's One+ plan, which costs $28.99 per month (discounted with an annual commitment) and includes a 30-day return policy. As Surfshark's premium offering, it encompasses standard VPN/AdBlock features as well as distinctive features such as webcam protection, antivirus, anti-spyware, malware protection, and data removal from company databases. Surfshark, a company I discovered through an advertisement, employs fear-based marketing tactics, collaborating with YouTubers to target the millennial/GenZ demographic. Upon reflection, I was struck by the realization of fear commodification. While I strive for objectivity in my research, it is increasingly challenging to ignore the exploitative sales tactics employed by companies like Surfshark, which capitalize on fear to sell products that are largely unnecessary and/or freely available through browser extensions or simple browser setting modifications. This highlights a significant gap in online security education, which companies are beginning to exploit.

Lockdown Privacy

Lockdown Privacy, developed by two former Apple security engineers, is a straightforward VPN client that prides itself on its open-source nature. It offers a free privacy firewall along with a paid VPN service. However, I found Lockdown to be costly for the services it provides. The perceived trustworthiness that Lockdown offers is commendable, and I believe that their service delivers on its promises, unlike the illusory privacy offered by other companies. One issue I encountered with Lockdown was its inability to allow me to use my iPhone as a hotspot for my Mac, a likely use case in situations with strong cellular coverage but insecure public Wi-Fi. As someone who frequently works in public spaces, this limitation quickly became a significant inconvenience.

Mullvad

Mullvad, the only VPN recommended by Sun Knudsen, piqued my interest. The enrolment process was fundamentally different from the others I had tried.

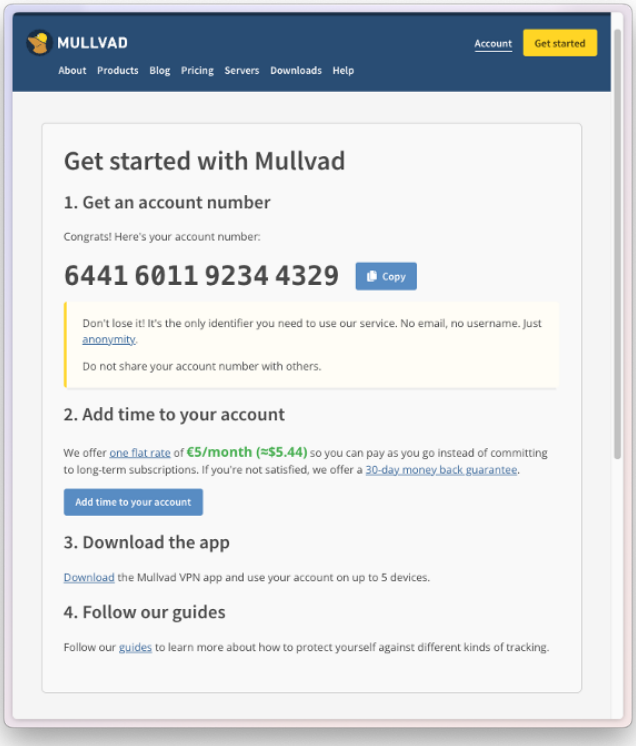

Figure 5: Mullvad's onboarding process, showcasing the simple nature of an inherently complex product.

Mullvad, based in Sweden, is subject to stringent privacy laws enacted by its government, in addition to the comprehensive regulations of the European Union (Mullvad, 2023). Priced at €5 per month for its only tier, Mullvad offers features comparable to larger, more ostentatious companies, but with one distinct advantage. Mullvad generates an account number for the user to connect with the service. The account can be preloaded with money using various payment methods, including card, PayPal, cryptocurrency, and even cash. This addresses a common issue faced by VPN providers and serves as a safeguard in the event of vulnerability breaches. Mullvad's balance of user understanding, and actual privacy needs is why I endorse Mullvad and will continue to follow their security recommendations and tools.

Private Relay

Apple's iCloud Private Relay presents an intriguing alternative to traditional VPNs, given that it technically does not qualify as one. It does not allow changing IP location and can be used in conjunction with a VPN. It functions by establishing two independent relays, thereby separating the IP address from the visited website (Apple, 2021). This framework can be found in traditional VPN clients as a feature known as "multi-hop". However, based on my research on several providers offering this feature, the consensus is that multi-hop connectivity is an advanced feature that most users will not require, and thus, it is often buried under other settings. Apple has highlighted an important concept known as the decoupling principle, which advocates for the separation of identity from actions (Schmitt et al., 2022). Although not flawless, iCloud Private Relay could potentially be the most suitable solution for a vast majority of individuals. In Canada, the minimum subscription requirement is a base iCloud+ tier offered by Apple, starting at $1.29 per month. iCloud+ also includes an email forwarding feature, which warrants further discussion.

Results of Research

Upon conducting a comprehensive evaluation of numerous Virtual Private Network (VPN) providers, I established that, barring certain specific

circumstances, the utilization of such services is largely superfluous for the average individual. These circumstances encompass scenarios such as the necessity to access geo-restricted content in a foreign region, or to circumvent restrictions imposed by governmental or institutional entities within one's current locale. In the context of the conducted evaluations and personal requirements, neither of these conditions were applicable. Consequently, the employment of a VPN client resulted in a diminished internet connection speed and potential financial implications. This necessitated further exploration, as the absence of a VPN was unsatisfactory, yet its usage proved excessively intrusive to habitual browsing practices.

An area of interest was the examination of the specific "features" offered by these VPN providers, and whether they could be replicated using an alternative service or feature that did not necessitate a subscription and would not be obtrusive. Surfshark, which boasted the most extensive array of "features", was selected for this analysis. Each feature was dissected and compared to a pre-existing product that could potentially serve as a substitute. At this juncture of the research, a sense of irritation emerged due to the commodification of fear that appeared to be a marketing strategy employed by the company. A notable feature, not included in Surfshark's base tier, was a search function promising "[a]d-free and completely private web searches to avoid tracking" (Surfshark, 2020). For a monthly fee of $19.99, this feature can be replicated at no cost simply by altering the default search engine on most contemporary browsers to DuckDuckGo, thereby providing a tracking-free experience with advertisements generated by search queries rather than online browsing algorithms. Other features encompassed webcam protection by disabling WebRTC through browser settings or via extensions. These, in conjunction with other features bundled with the Surfshark subscription, underscore the unnecessary nature of VPN providers. A configuration featuring Mullvad's VPN, coupled with a few modifications to browser settings and a selection of browser extensions, can equate to a significantly more economical and potentially robust privacy solution.

From a design perspective, VPNs are tricky. They are objectively complex pieces of software that aim to do very technical changes that most end users would just nod and smile at. Credit where it is due, Surfshark does a great job of elaborating on its core features and what they do along with having an intuitive interface once installed. However, I questioned before whether the product needs the user, or the user needs the product. I implore VPN providers to look at examples from Apple's Private Relay, which provides similar privacy protections as a full-fledged VPN but without the visual clutter and complex onboarding; it just works, and I don't have to think about it. For users to think differently about their privacy, the barrier to adoption needs to be as low as possible. Mullvad provides a great onboarding experience yet manages to be the most secure of the VPNs tested, putting anonymity first yet making it easy. There is a sense of trust out the gate. I want to see more transparency when it comes to feature sets from VPN providers and to understand that snake oil is easy to spot with a quick search and the right set of eyes.

Dispersing Your Data

A central theme I discerned pertains to the dispersion of one's identity from traceable variables, encompassing elements such as the decoupling principle, passkeys, and email forwarding. It is crucial in the big picture of data privacy to understand how our digital data roams across a plain we cannot see. Having the ability to find our own data and then decide what to do with it is powerful – yet it shouldn't be. It is ours, we/I/you produced it. Why are we then conditioned to be so willing to give it out when it is asked for, when that would rarely happen on the streets of Vancouver or at our local coffee shop. I wanted to explore ways a user could have more control over the data they produced and find solutions or tools that could help mitigate the triangulation of online identity.

The advantage of an email forwarding service like iCloud+ lies in its ability to segregate your private email from a website or service. By generating unique email forwarding addresses, the dissemination of your personal information can be curtailed by offering a randomly generated email that can be forwarded to an

email of your choosing and can be instantaneously deleted. This also safeguards certain aspects of personal identity in the unfortunate event of a data breach, such as the 2018 breach of MyFitnessPal, which exposed 144 million user emails, passwords, and IP addresses (Hunt et al., 2019). The problem is twofold, as leaked user emails pose a risk of exploitation if they are used for other sites. A fascinating report from cybersecurity firm SpyCloud examined various combinations of already leaked email and password combinations (1.7 billion were discovered) and found that 64% of individuals used the same password exposed in the 755 leaked sources (Tung, 2022). While the data is from already leaked sources and cannot extrapolate valid data, the trend that a significant number of passwords, and presumably emails, are used repeatedly among websites thus one singular breach could expose many other vulnerabilities. The security breach of MyFitnessPal seems to not include any sensitive health data and no payment data was retrieved either. I was part of the data leak.

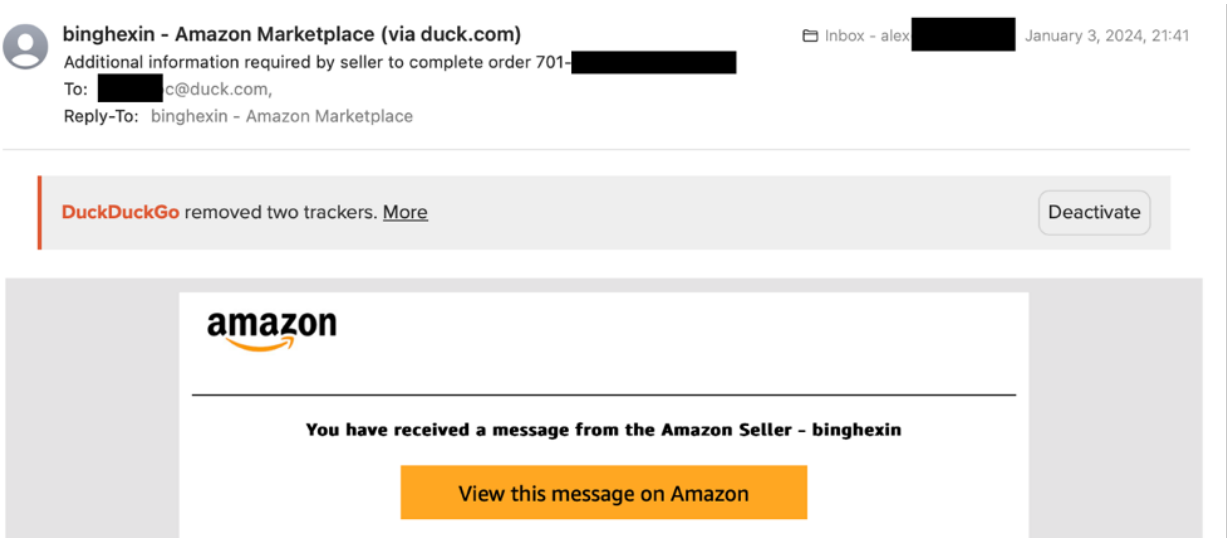

Figure 6: An example of DuckDuckGo email forwarding, highlighting a seamless integration with regular mail.

Email Forwarding

Several services currently possess the capability to forward email via a "burner" email, with iCloud+ and DuckDuckGo being examples. Founded in 2008, DuckDuckGo espouses a privacy-first philosophy for search engines, eventually

leading to a browser extension and a standalone browser. Essentially utilizing a browser's private-browsing window by default, DuckDuckGo does not track its users, instead serving ads based on the search query made (Duck Duck Go, Inc., 2023). Observing the increase in email trackers from brands and companies, Duck initiated their email forwarding service in July 2021, enabling users to claim an "@duck.com" address and have emails forwarded to their personal email with the trackers stripped.

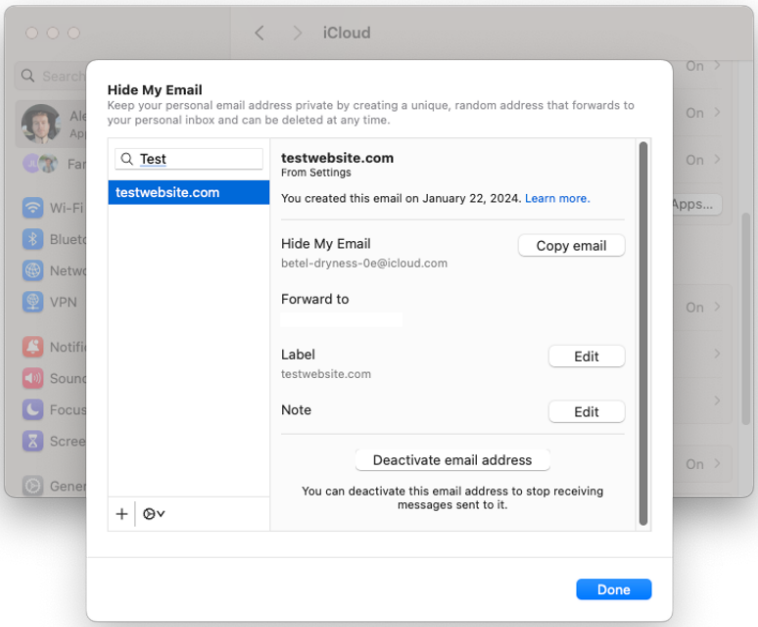

Figure 7: Apple's Hide My Email, part of an iCloud+ subscription; an effective method of protecting online identity.

While other providers like Surfshark may charge for this service, Duck provides this for free. The primary benefit of having an email forwarding service is the disposability aspect of the email; if the email were to appear in a data leak or simply become a nuisance (from spam or overly excited marketing teams, for example), it can be easily deleted and replaced with a new one. The initial setup can result in an increase in user involvement, but the time saved down the road could make the investment worthwhile. This method, however, is not without

caveats. Firstly, an email set up through a forwarding service like iCloud+ cannot be used to send emails, an issue I have encountered several times when dealing with customer service agents for online shopping. Using Hide My Email allows the user to reply to an email sent to them, but they are unable to initiate a conversation directly from the generated email. Duck does not allow replies at all. Secondly, generated emails can accumulate quickly, leaving a laundry list of unique addresses that are only really known by the list stored in iCloud. Again, Duck does not have such a list. If a user forgets the email to an account using a generated email, it could be difficult or impossible to recover the login credentials. For these two reasons, email generation via Duck can only really be recommended for newsletters that won't ever need to be responded to – iCloud+ has a more usable system with their Hide My Email, albeit with a cost.

The Decoupling Principle

The principle of decoupling can be applied in numerous scenarios, primarily because the fundamental concept remains consistent – separate data between two distinct entities. If one entity is compromised, the other remains secure. As per Schmitt, Apple's Private Relay closely aligns with, but does not perfectly embody, the decoupling principle, given that Apple must adhere to specific use cases such as DRM (Digital Rights Management) requests from streaming services to geolocate a user. While such requests can maintain user privacy, they nonetheless violate the principle. Passkeys represent a novel password-less standard, founded on the FIDO Alliance and W3C, two leading entities in internet authentication standards. By decoupling your login into a cryptographic key pair, comprising one public key for the website and one private key for the user, passkeys facilitate the creation of credentials that are impossible to guess or reuse, given that each passkey is associated with a specific site, thereby rendering every cryptographic pair unique. Passkeys are starting to show up across the internet, and a current list of supported sites can be found here.

Garden Thoughts

Dispersing one's identity can be a challenge because it is a culmination of many different products and services. While Apple is not the saving grace in this situation, they do offer the best suite of built-in tools and services that other companies and manufacturers may struggle to compete with. This could simply be because of the top-to-bottom integration of Apple's software and hardware allowing deeper integration with OS-level features. While I fully acknowledge that following the path to Apple is locking oneself into a "walled garden", it is hard to ignore the privacy benefits and intuitiveness of the garden. It is difficult to make design recommendations outside of Apple because the business model of their competitors stifles such efforts to meaningfully boost privacy for its users in a way that would have the barrier of adoption low enough for most users to follow through with enabling privacy-focused features and settings.

There are many ways to secure non-Apple devices, arguably easy to do so. The reasoning behind the lack of recommendation is the common thread throughout this research, the barrier to adoption is simply too high for an everyday user to enable privacy-related features in a way that would make a meaningful difference for me to recommend. Simply for curiosity's sake, I had tried to break out of the garden and try a Google Pixel – it lasted about two days. Without too much detail, here is the shotgun review and why I went back: illusion of choice is deeply rooted into the whole experience to the point of it being overwhelming, a suspiciously large amount of accepting (mostly declining) very long terms and conditions or poorly worded and convoluted requests for data usage, and a lack of trust when it came to Android OS and it's usage of what it was collecting and the inability/difficulty to stop it. Securing non-Apple devices are "arguably easy to do so" because it is easy to tweak and download bits and bobs to truly lock down and protect a device in a way that wouldn't be possible on an Apple device. During my two-day stint however, I couldn't help feeling as though Google did not want that to happen in the nicest possible way.

Is a VPN the Best Solution?

As stated, the purpose of a VPN in a use case like mine is for strong protection against external threats. There is little-to-no interest in accessing Netflix from Brazil, nor a need to login to corporate networks. Realistically, a VPN is unnecessary to the point of being obtrusive, thus another solution would be ideal. The use of browser extensions and application tinkering can get close to a feature set that a provider like Surfshark offered, but missing is the secure tunnel in which a VPN provides. One strategy to substantially increase privacy while browsing on the web is to utilize Hypertext Transfer Protocol Secure, more widely recognized as https://. Built as a "secure" version of the standard http://, https:// uses an encryption protocol to increase security of data transfer. It does so by utilizing a protocol known as Transport Layer Security (TLS), using two different keys to encrypt communications between two parties. Another potential example of the principle of decoupling.

The key benefit of using https:// is that it shows the user that the site they are visiting is the site that was requested, and traffic that flows between the user and the site cannot be sniffed out or intercepted. The downside, however, is that https:// only applies to websites you visit in a browser, they do not apply to internet traffic made outside, such as mobile applications. For internet browsing on a desktop or laptop computer, this is less of an issue, as most of a user's interactions occur within the browser. For mobile, applications dominate the home screen, therefor unable to go through the https:// protocol set in the browser. A simple workaround exists however, thanks to Mullvad.

DoH-Re-Mi

While selling their VPN to customers that may need such a tool, Mullvad also provide a free solution to browse securely on multiple different devices. They do so by using what is known as DNS over https:// (DoH). A DNS, or Domain Name System, is essentially the phone book of the internet. The name is the websites name, such as bbc.com, and their "number" is the IP address where the website is

located. DNS by itself isn't secure, as everyone has the same phonebook and can look up who owns the address. The use of DoH is simply that instead of every party using the same phonebook, you are putting your specific phonebook in an envelope for your receiver to open, nobody else. This encrypts your request through the internet. This solution is great because it does this process for all internet traffic coming off the device, not just from a browser using https://. It is also a set-and-forget process, since it is installed on the system level, it is on and always on and doesn't need to "boot up" like a VPN client would. It is important to note that DoH does not hide ones IP and is still visible to the website you are visiting and your internet service provider (Shaw, Telus. etc.).

When Privacy Falls Short

It is essential to acknowledge that all efforts to enhance user privacy do not always yield successful results. Part of my research involves looking at the great feats that can come with robust data privacy, but learning from faulty or lacklustre experiences is important to learn from and develop a better understand of user needs and wants. I needed to discuss scenarios where the outcome was less than ideal, because new technologies are becoming available and evolving rapidly. A notable example of this is the App Tracking Transparency (ATT) initiative, introduced by Apple in 2021. The primary purpose of ATT is to provide users with the option to opt out of app tracking on iOS, thereby creating a more transparent relationship between the user and the company attempting to track.

A study led by Johnny Lin and Sean Halloran, the founders of Lockdown Privacy VPN and former Apple engineers, found that the number of active third-party trackers remained unchanged and had little to no impact on tracking attempts (Lin & Halloran, 2023). This was discovered when apps were initially onboarded and tracked using Lockdown Privacy, once when selecting "Ask Not to Track", and another time when ignoring the prompt. Using the Lockdown Privacy app on iOS, they found negligible differences between the two scenarios,

concluding that ATT was functionally ineffective. Apple, a pioneer of many privacy-focused initiatives, has unfortunately fallen short with App Tracking Transparency. Hypotheses can be formulated regarding the reasons for this shortfall. Arguably, Apple has no incentive to regulate the App Store, given that it constitutes a significant portion of their revenue, and they receive a 30% cut from all purchases made in and through their App Store. This situation contrasts with first-party apps and their specific privacy policies. With a recent software update, Apple introduced Advanced Data Protection, making a significant portion of Apple's services end-to-end encrypted, meaning not even Apple can read the data being transmitted.

The perception of privacy when it comes to first party (made by Apple) versus third-party (not made by Apple) applications is where ATT falls short, as it provides a false sense of security to a user who may be accustomed to a certain standard of privacy when using an Apple device. I want Apple to more rigorously vet the content that is uploaded onto the App Store for better data protections and take actions when an application is overreaching the perceived trust it bestows upon its users. The UI elements are already there, and applications like Safari already do this. Prompting the user about App Tracking is a truly great feature to help with the understanding of privacy, it just needs to be implemented in a way that isn't an empty promise. The development of Data Wallet was inspired by this very idea of ATT and has the feasibility to exist in iOS for users to view data transactions much like financial or location data.

The feasibility of Data Wallet came into question when I started to look into how it could be realistically implemented in an operating system and what it would require from the users and developers alike. Most users simply do not understand where their data is going, and Data Wallet aimed to showcase the transactional element of that process. However, it was under the assumption that the Wallet had access to such data and could provide the user with the ability to block and/or restrict data going off the device; an inverted toll booth, let's say. Having such power from the user may not bode well with app developers who rely

on these invisible transactions - the irony. Looking at the scale and funding behind Apple, implementing a feature like Data Wallet into their next WWDC sounds simple enough.

The development of the app isn't the challenging part however, forcing developers to go through the toll booth may not be a welcome change and will require a strong hand and unwavering commitment to user privacy at the expense of business relations. As a user, it is evident that using my digital data as bartering chips in the exchange of vast wealth among large corporations is not something I am particularly fond of. Realizing the assumptions required to turn Data Wallet into a reality, I wanted to investigate how I could still give power and autonomy to users without needing to bend for others. In Privacy Toolkit, I explore how on-device changes could be made or enabled to protect a user's data without requiring the acknowledgement of third-parties.

It's Not You, It's Them

In October 2023, the Pew Research Center (PEW), a nonpartisan and non-advocacy fact tank renowned for conducting public opinion polling and demographic research, published a report entitled "How Americans View Data Privacy". This comprehensive study surveyed 5,101 U.S. adults, exploring their personal perspectives on privacy, data, and online habits. A salient observation revealed in the report was the apparent correlation between educational attainment and attitudes towards data privacy. Specifically, individuals possessing a High School diploma or less expressed greater confidence in the appropriate use of their personal data by those who had access to it and demonstrated a more relaxed attitude towards privacy (McClain et al., 2023). This contrasts with the attitudes of individuals who had attained at least a college degree or higher.

The report did not delve into the reasons behind this observed phenomenon. However, it is intriguing to note that a higher level of education seems to correlate with an increased awareness of privacy issues and a decrease in confidence in the data management practices of companies. The surveyed individuals were not

queried about their specific degrees, suggesting a diverse range of specialties within the group. This diversity further amplifies the interest in understanding how and why post-secondary education leads to heightened privacy awareness, even in the absence of explicit privacy-related curriculum.

Reflecting on my high school experience in the early 2010s, data privacy was neither a topic of conversation nor part of the educational curriculum. This could be attributed to a simple lack of necessity at the time. Security features such as two-factor authentication were not widespread, as many students, including myself, did not possess a cell phone, and the surge of social media was just beginning. Fast forward a decade, and the landscape has dramatically changed. As of 2019, 84% of American teenagers now own cellphones (Kamenetz, 2019). The PEW report only surveyed individuals aged 18 and above, yet over half of American children possess a smartphone by the age of 11. The rapid adoption of smartphones and the consequent expansion of the data pool available for companies to harvest underscore the critical importance of incorporating privacy and data education into the school curriculum.

However, the challenges do not end there. Companies like Facebook are leveraging the extracted data to create complex algorithms that construct digital identities of their users, encompassing vast amounts of data that are difficult to comprehend. This development further emphasizes the need for robust privacy education and awareness.

> God View refers to the comprehensive perspective that Big Tech companies have on individuals' behaviours and experiences due to the extensive data they collect. (Zuboff, 2019)

Uneasy Lies The Head That Wears The Crown

Zuboff's interpretation of the "God View" concept, in conjunction with the revelations from the Cambridge Analytica scandal, paints a disconcerting picture of the future. The stranglehold that Big Tech companies exert over their users is progressively tightening, fuelled by an expanding understanding of their

respective "God Views". The scandal that unfolded in 2018 was not merely an exposé of data harvesting practices; it offered a glimpse into the formidable power of data in crafting user algorithms and constructing online identities. It was revealed that a substantial portion of the harvested data was linked to political affiliations, including those of former President Donald Trump and Senator Ted Cruz, as well as the Brexit referendum. What began as a platform for connecting with loved ones and engaging in casual games like FarmVille has morphed into a potent force in politics and policy.

Social media now controls the algorithms that dictate the content users see, potentially swaying their perspectives from behind an invisible veil. Our online data is evolving beyond mere IP addresses and phone numbers; it is transforming into a digital persona that mirrors our real-world selves. This persona is used to predict our behaviours and actions before we even make them, underscoring the profound influence and reach of these digital platforms.

Quick! Nobody Is Looking

Exploring how law and order influence data privacy is crucial for my own research. Understanding ways a user can protect themselves cannot be understated, but this a dance and we need a partner, data privacy laws. Players like the EU have had immense impact on shaping privacy protections, enough to force change upon how Silicon Valley view and produce products and services. A discerning reader may observe that a significant proportion of discourse related to privacy emanates from the United States, the home of Silicon Valley. Google and Meta, two entities identified by Zuboff as potential threats, are situated in proximity in California. One could hypothesize that there is something unique about the air in California, but a more disconcerting theory could be at play (without undermining the significance of air).

The United States lacks comprehensive statutory data protection laws, leading to inconsistencies across state boundaries as each state may have

divergent and potentially conflicting laws, leaving citizens in a state of confusion and potential vulnerability. This lack of uniformity extends to the global stage, with the United States, along with China, Saudi Arabia, and India, being the only G20 nations without statutory data protection laws. This stands in stark contrast to the European Union, whose laws have served as templates for legislation worldwide. The General Data Protection Regulation (GDPR) enacted by the EU has become the gold standard for data protection. Spin-offs of this regulation include the Consumer Privacy Protection Act (CPPA) in Canada and the California Consumer Privacy Act (CCPA).

The impact of the GDPR is profound because it empowers consumers by holding companies accountable for their handling and treatment of personal data. The GDPR does not take lightly to irresponsibility; of the 20 largest fines imposed by the GDPR to date, Meta features in seven of them. These include a €405 million fine for concerns over the processing of children's data and a €1.2 billion fine for transferring personal data of European users to the United States without adequate data protection measures in place (Data Privacy Manager, 2023).

The General Data Protection Regulation (GDPR) is a comprehensive data privacy law implemented by the European Union that provides individuals with control over their personal data. It imposes strict rules on those hosting and processing this data, anywhere in the world, and applies tough penalties for those organizations that fail to comply with these rules.

The influence of the GDPR cannot be overstated, and it is challenging to envision its implementation in a country like the United States. Given their dependence on data collection and processing, U.S. tech companies could face significant repercussions under GDPR-like regulations. The views of citizens may also vary, given that freedom of speech and commerce are deeply ingrained in society. Due to the complexity and potential impossibility of implementing a GDPR-like policy guideline in the United States, it falls upon its citizens to cultivate their own sense of data privacy and knowledge.

Providing citizens with a simple framework of what data privacy laws are applicable to them would be great to expand upon. Canada provides a general

template for the breakdown of *Personal Information Protection and Electronic Documents Act (PIPEDA)*, but in typical legal jargon that is not interesting nor engaging to read. Developing a website that allows citizens to see what they can do to protect themselves and what services and help are provided against potential breaches in data privacy would be a good start. Providing details on what it means to use a US-based service would also be welcome, as the difference in US versus Canadian-based data servers are potentially not well understood.

What Now

I Don't Care

Fair. It is understandable to not care about something that is hard to understand and impossible to see. It happens all around us and we perhaps link it to just coincidence, when we chat with friends about the next summer vacation and then suddenly receive an influx of ads from travel agents or airlines the following day. The things we do online have an impact on anything and everything, it depends on who wants to know. Understand that online data as a form of currency in the biggest marketplace known to man (Eggers et al., 2013). It's used by companies to target ads, improve products, and even sold to third parties. If you don't control your data, you're giving away something valuable for free.

You may not even have the choice to give it away. In the United States, identity theft is a significant issue. According to the Federal Trade Commission, Georgia had the highest number of identity theft reports per capita in 2022, with 574 reported cases per 100,000 residents (FTC, 2023). The most common being credit card fraud with bank fraud, loan or lease fraud, and phone or utilities fraud also on the list. Simple practices can be implemented to minimize or prevent potential theft or fraud like browsing on a website using https:// and not using public Wi-Fi for sensitive information.

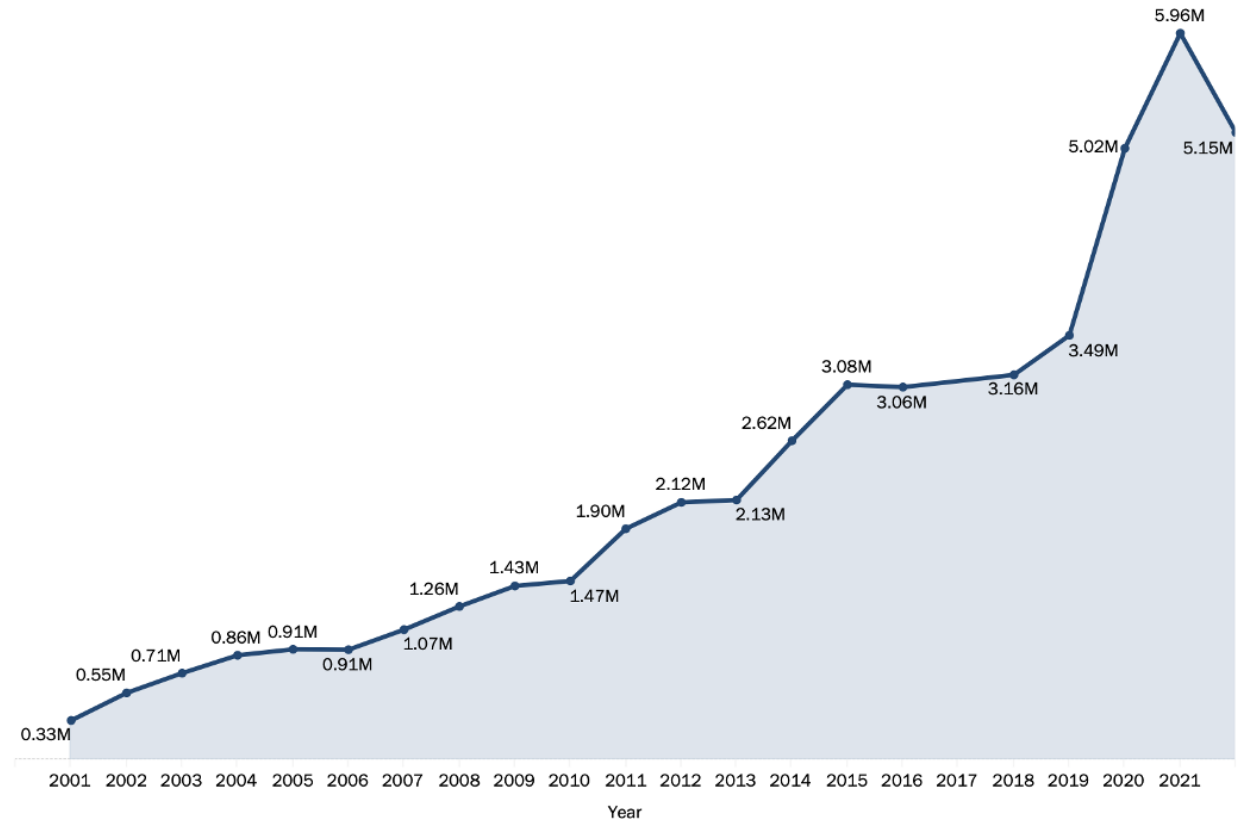

Figure 8: Number of Fraud, Identity Theft and Other Reports by Year (FTC, 2023). A substantial increase from the early 2000s.

Privacy Toolkit

The unnecessary complexity and high barriers of understanding of modern technology lead many consumers confused about their own privacy, even for companies that provide simplified marketing terms to break it down. On Apple's Safari, the "Privacy Report" highlights trackers prevented from profiling your browsing. On Microsoft Edge, a feature called "Secure Network" encrypts user's web traffic using a Cloudflare-powered VPN service. Many similar features appear in many similar products, but what differs is if a user knows or cares enough to enable them. The harsh reality is that as discussed, data has extraordinary value to those who know what to do with it. Those who know what to do with it are great at making products with such vast amounts of data to learn from and have little incentive to stop collecting such a valuable commodity. It is crucial forconsumers to have the access to privacy knowledge they can use to decide how

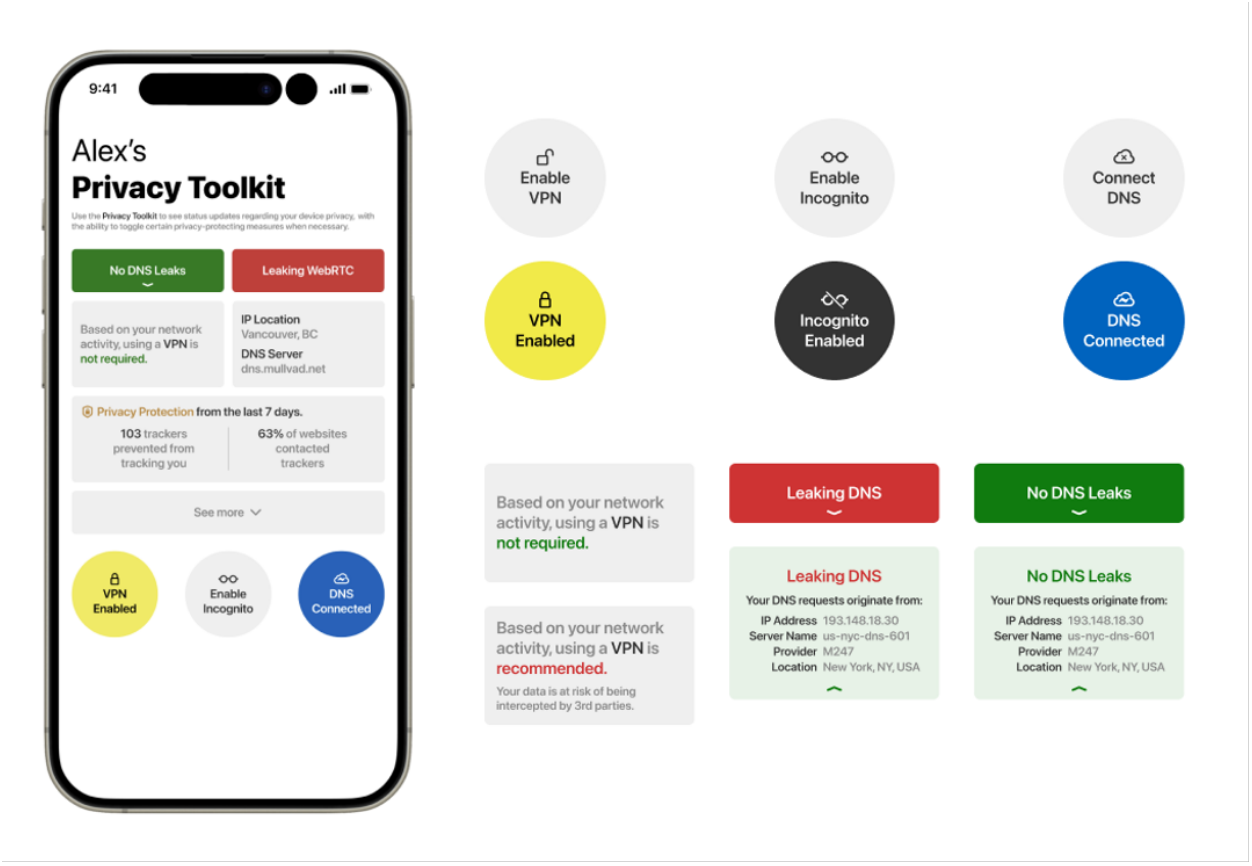

Figure 9: Privacy Toolkit - replacing Data Wallet to view data as a system status rather than a value proposition.

they would like to proceed navigating such rocky terrain, and I wanted to explore ways to visualize settings or tools that a user could view and have a general understanding of what they do or mean. After learning about potential blockers with Data Wallet, specifically knowing that using Apple's ATT is not a reliable source for information and the large assumptions necessary to make the product functional, I wanted to explore a simpler way of visualization.

The goal of Privacy Toolkit is to provide a simple way to view complex information. Merging privacy features from various software along with system-level operations, navigating privacy settings should be a simple process. VPN and DNS toggles are at the forefront rather than being buried in settings on typical devices, along with quick information tiles updating the user on the status of their security. As this is iOS focused, the "Privacy Protection" is built from Safari's own feature but brought down to a system level.

Figure 10: An example of a Siri Shortcut that alerts you when connected to Public WiFi.

The reason I chose to focus on an iOS direction is because their business model is from products (like iPhones) and services (like iCloud) rather than ads. The implementation of such a feature is more likely to occur than on an operating system such as Google's Android OS. One thing I have noticed repeatedly is how a user may say to me that privacy is not a huge concern for them, I cannot help but wonder why that is the case. When an iPhone connects to a public Wi-Fi network the only prompt is that the connection is insecure, assuming that part is even read. There is no indication as to what you should(n't) do on an unsecured network, so those connecting to it will go about their usual business. There is a distinct barrier when trying to access a website that is not https://, and the user is explicitly asked if they want to continue. This is great, why stop there?

In the case of Apple's iOS and MacOS, there are multiple privacy features built right into the software but are hidden away, like an optional feature turned

off by default called Advanced Data Protection. By opting for Advanced Data Protection, you ensure that most of your iCloud data, such as iCloud Backup, Photos, Notes, and more, is safeguarded through end-to-end encryption. This level of security means that your encrypted data is inaccessible to everyone else, including Apple. Moreover, even in the event of a cloud data breach, your information remains secure.

Ghost in the Shell

Throughout this research, my perception of what I am seeking was unknown. I think I wanted to be safer online and protect my digital identity from potential threats and hacks. I think I wanted to have my guards up and guns loaded in case a breach occurred. I think I wanted anonymity. Now however, I understand that anonymity was never the goal. I am not running a criminal organization nor hiding from government entities, yet I set myself up in a way so that I could run a criminal organization and hide from government entities. Why? "I have nothing to hide..." is a familiar sentiment I have heard in recent months, and it is indeed true - I don't. However, privacy needn't be a switch of on or off. Becoming a ghost on the internet was never my intention, yet I am led to believe from security-related marketing that if I do not become a ghost, I am at risk of cyber-attacks and identity theft - I must hide my IP address and I must delete my cookies after every browsing session.

Truth be told, I don't want to. If I am on DuckDuckGo and searching for places to eat, I would prefer it to know my location and show me restaurants around me. I would prefer to not log into YouTube every time I open it and use two-factor authentication to watch videos. Being anonymous while searching for tonight's dinner is more of a pain than a benefit in this way. Throughout my research I was not seeking anonymity, I was seeking solitude. I want the power to step away from the connectedness when I choose to. I want to be in my own little cubicle of the internet, shutting the blinds when I require.

This became evident to me when I had the personal experience between solitude and anonymity. As a member of the LGBTQIA+ community, there are times when my physical identity is a shell that I may need to adapt or change within the context of my surroundings. Travelling to Idaho with my partner, I had an indescribable sense of eeriness walking around the various spots we visited; a feeling I have yet to experience while living in Vancouver. Discovering that Idaho was a GOP stronghold, the sense of fear clouded over once I felt like an outsider for possibly the first time in my life. Being in an interracial same-sex couple was something that never had me thinking until it became "unusual".

In this context, I couldn't be anonymous, I wanted to go eat out with my partner and enjoy the activities and amusement parks, the reason we went at all. My identity that I had taken for granted as intertwined with my being had now suddenly become a shell, be slightly more masculine and slightly more heterosexual. I craved solitude at that moment. I wanted to feel safe, I wanted to keep my partner safe. Everything became so immersive, feeling the eyes staring at the back of my head while I acted less than myself. This is real and I could feel it. I cannot see the eyes online. I cannot feel the discomfort online. My physical and digital identity are perceived differently. Sometimes I feel as though my online presence is a digitization of Idaho, but it is midnight, and everyone has night-vision goggles apart from me.

What I struggle to convey is that the world wide web is not anonymous. I sit on my sofa writing this work and saving it to iCloud Drive, searching Duck for resources via Private Relay and storing them locally on Zotero. I can imagine that anyone trying to break into my digital life to obtain this document may have a slightly challenging time to do so. This is the bare minimum. I want to live in privacy, but I want to live with some level of convenience. This is a culmination of research and adaptations to workflows, enabling settings and disabling others. Paying for features that protect me and being cognizant where I step. Others may not. Others may be told to be a ghost or get hacked. Pay for services or get their identity stolen. Buy this or have bad outcome. This is fear mongering, this is dirty

marketing. Enabling DoH is free, enabling Private relay is free* (if paying for iCloud storage for $1.29/month), using digital payment methods over physical cards is free. The barrier to security is rarely due to cost, it is the lack of information.

#OwnYourData

Being aware of what data you produce and where it goes sounds tricky, but it needn't be. It becomes complicated because ad companies make it that way in what is known as "dark patterns" in design (Nguyen, 2023). The act of opting out of cookies becomes challenging but accepting all cookies is a single click, creating a new account takes multiple steps or simply Sign in with Google. Being cognizant of how websites and applications are designed can help you understand what the main objective is with the product.

Data privacy from a consumer perspective may feel like being a plankton in an open sea - we're dealing with powers far bigger than what we can handle. It may even feel helpless to even start trying. It is up to the everyday consumer to have the tools and resources to protect themselves against malicious design practices and abusive data harvesting - whether that be reducing/eliminating the use of applications designed by Big Tech, supporting independently owned companies and accepting that a potential cost will occur regardless; whether that be a financial cost or personal cost. The pivot away from Data Wallet was for this very reason, it expected too much from companies; I wanted to focus more on what consumers *could* do rather what companies *should* do.

The goal is not to become anonymous; it is to simply be aware. Providing the tools and resources to be able to dictate how you want your data to be used. If using Google and banking on Starbucks Wi-Fi is convenient for you, go for it. Data is becoming the most valuable currency we have ever been able to transact with. Understanding that your data has value and weight in different hands is critical, make them work for it.

Bibliography

Apple. (2021). iCloud Private Relay Overview. Learn how Private Relay protects users' privacy on the internet. Apple. https://www.apple.com/privacy/docs/iCloud_Private_Relay_Overview_Dec2021.PDF

Confessore, N. (2018, April 4). Cambridge Analytica and Facebook: The Scandal and the Fallout So Far. The New York Times. https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html

Data Privacy Manager. (2023, September 19). 20 biggest GDPR fines so far [2023]. Data Privacy Manager. https://dataprivacymanager.net/5-biggest-gdpr-fines-so-far-2020/

Duck Duck Go, Inc. (2023, November 5). We don't track you. https://duckduckgo.com/privacy

Eggers, W. D., Hamill, R., & Ali, A. (2013). Data as the new currency. https://deloitte.com. https://www2.deloitte.com/content/dam/insights/us/articles/data-as-the-new-currency/DR13_data_as_the_new_currency2.pdf

FTC. (2023). 2022 Consumer Sentinel Network Data Book. Federal Trade Commission. https://www.ftc.gov/system/files/ftc_gov/pdf/CSN-Data-Book-2022.pdf

Hunt, T., Hunt, C., & Sigurðarson, S. J. (2019, February 21). Have i been pwned? PwnedWebsites. https://haveibeenpwned.com/PwnedWebsites#MyFitnessPal

Kamenetz, A. (2019, October 31). It's A Smartphone Life: More Than Half Of U.S. Children Now Have One [News]. Education. https://www.npr.org/2019/10/31/774838891/its-a-smartphone-life-more-than-half-of-u-s-children-now-have-one

Lin, J., & Halloran, S. (2023, November 30). Study: Effectiveness of Apple's App Tracking Transparency [Blog]. Transparancy Matters. https://blog.lockdownprivacy.com/2021/09/22/study-effectiveness-of-apples-app-tracking-transparency.html

McClain, C., Faverio, M., Anderson, M., & Park, E. (2023, October 18). How Americans View Data Privacy. Report: Online Privacy & Security. https://www.pewresearch.org/internet/wp-content/uploads/sites/9/2023/10/PI_2023.10.18_Data-Privacy_FINAL.pdf

Mehrotra, D., & D'Anastasio, C. (2019, October 16). The Creators Of Pokémon Go Mapped The World. Now They're Mapping You. Kotaku. https://kotaku.com/the-creators-of-pokemon-go-mapped-the-world-now-theyre-1838974714

Meredith, S. (2018, April 10). Facebook-Cambridge Analytica: A timeline of the data hijacking scandal. CNBC. https://www.cnbc.com/2018/04/10/facebook-cambridge-analytica-a-timeline-of-the-data-hijacking-scandal.html

Meta. (2023, February 1). Meta Reports Fourth Quarter and Full Year 2022 Results [Press Release]. Meta Investor Relations. https://investor.fb.com/investor-news/press-release-details/2023/Meta-Reports-Fourth-Quarter-and-Full-Year-2022-Results/default.aspx

Mullvad. (2023, February 26). Swedish legislation relevant to us as a VPN provider. https://mullvad.net/en/help/swedish-legislation

Nguyen, C. (2023, July 3). 7 Dark Patterns in UX Design: A Guide To Ethical Design. A Better UX Career, Faster. https://uxplaybook.org/articles/ux-dark-patterns-and-ethical-design

Orvill, S. (2024, January 13). Pokemon Go Player Count, Revenue & Stats 2023. Pokemon Go Stats. https://prioridata.com/data/pokemon-go-stats/

Schmitt, P., Iyengar, J., Wood, C., & Raghavan, B. (2022). The decoupling principle: A practical privacy framework. Proceedings of the 21st ACM Workshop on Hot Topics in Networks, 213–220. https://doi.org/10.1145/3563766.3564112

Schneier, B. (2016). Data and Goliath: The hidden battles to collect your data and control your world (First published as a Norton paperback 2016). W.W. Norton & Company.

Surfshark. (2020, December 9). How much does Surfshark cost? Check the pricing. Surfshark. https://surfshark.com/pricing

Tung, L. (2022, March 3). We're all still using the same passwords, even after they've been breached. https://www.zdnet.com/article/were-all-still-using-the-same-passwords-even-after-theyve-been-breached/

Williams, M. (2021, June 29). What's the truth about the NordVPN breach? Here's what we now know. Techradar Pro. https://www.techradar.com/news/whats-the-truth-about-the-nordvpn-breach-heres-what-we-now-know

Zuboff, S. (2019). The age of surveillance capitalism: The fight for a human future at the new frontier of power. Profile books.