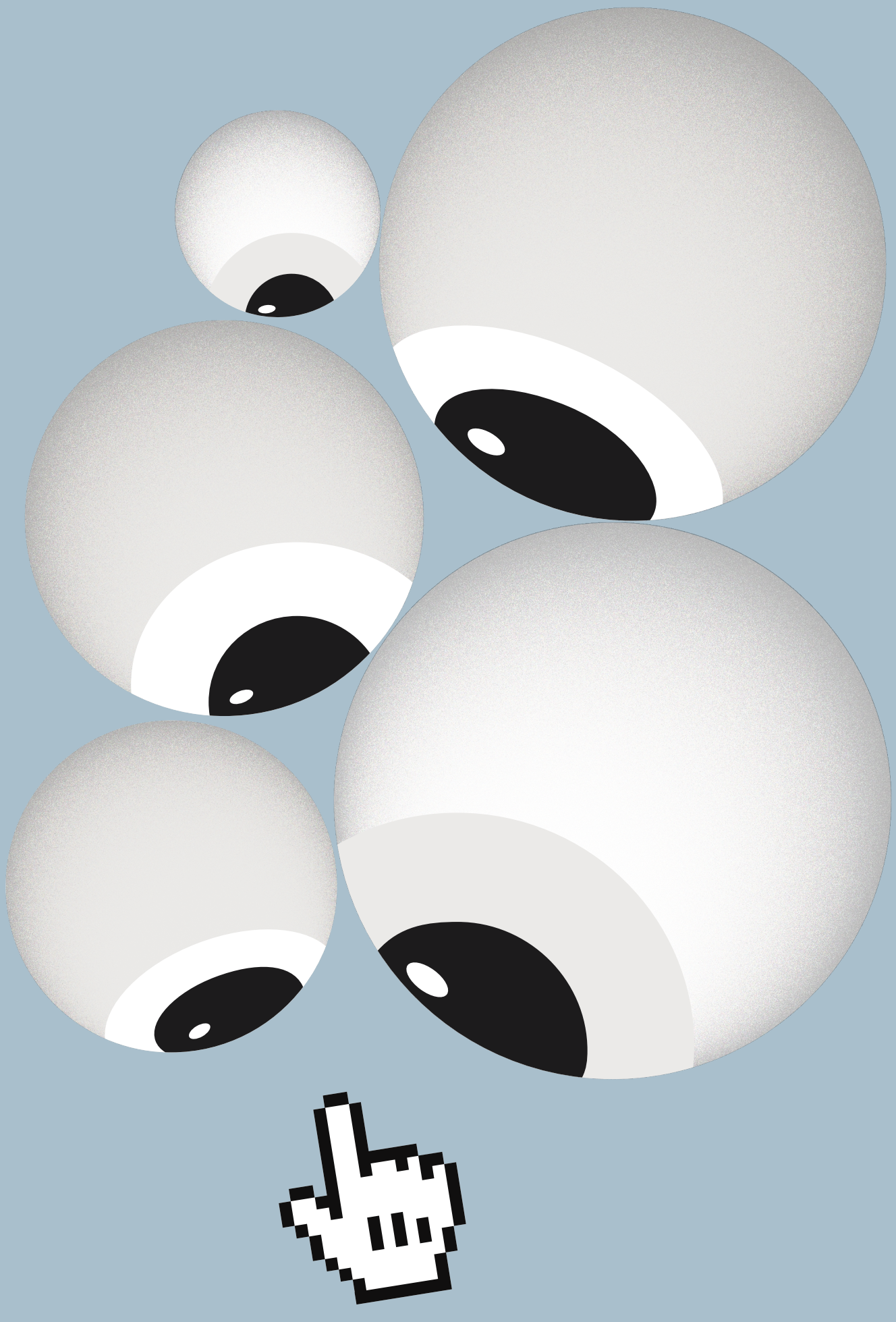


Data Aeternum

A guide to Data Privacy: What it means for you, Why you should care, and How to take back control.

Get Actionable Steps:
data-aeternum.com

Table of Contents

Get Actionable Steps:
data-aeternum.com

Ch 01.

Introduction

Introduction

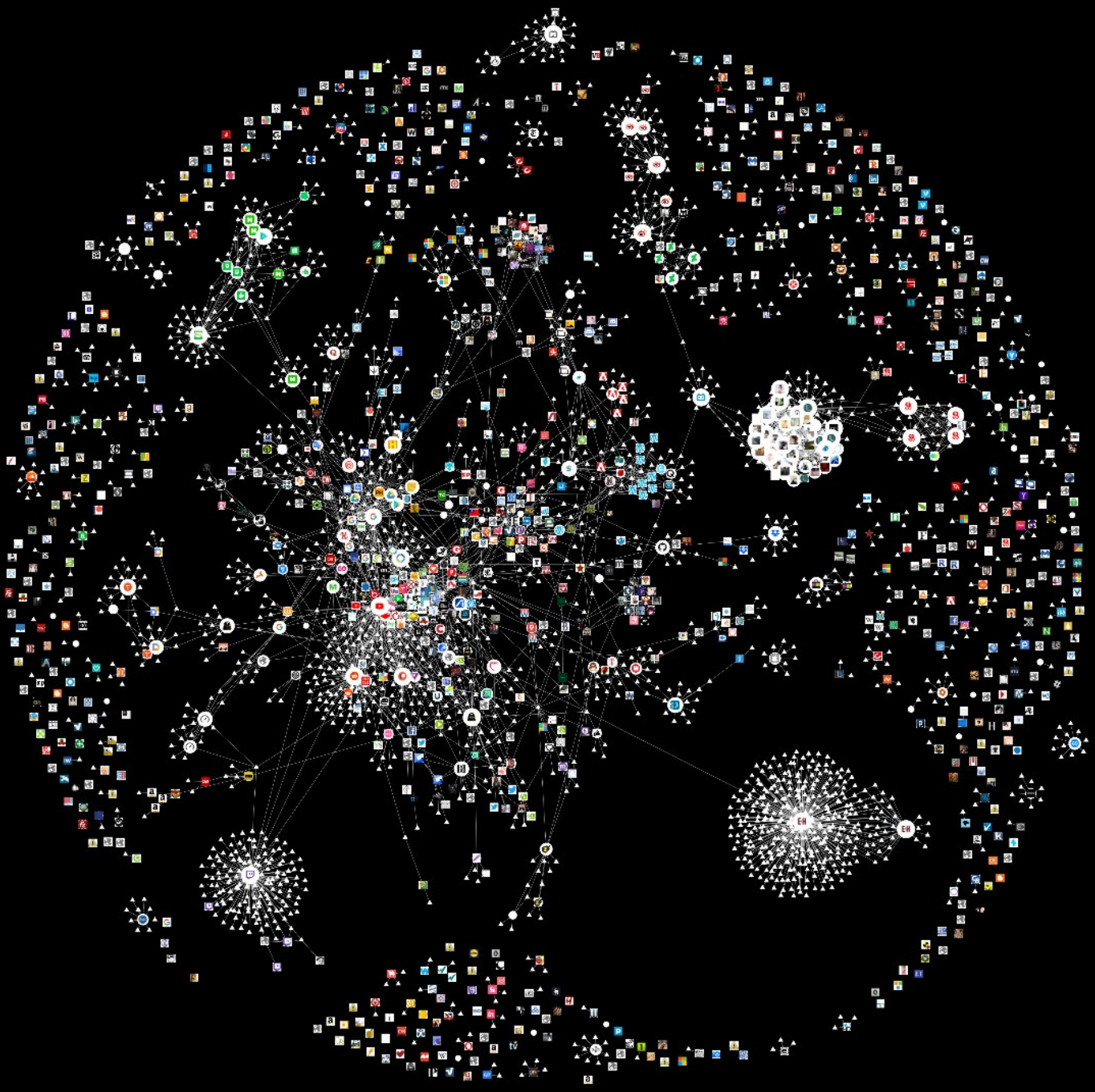
Welcome to Data Aeternum! Let's talk about something you rarely think about—Your Data Privacy. Chances are, instead of reading this, you actually want to be on Instagram, seeing all the "grammable" things your friends are doing, or on Facebook, looking at cute puppy videos. You sure haven't checked Twitter in a while, what's the most recent hashtag that's trending? Oh, and look, your favourite Youtuber just uploaded another video, for the 6th time this week.

With all of these platforms (and countless more) constantly fighting for your attention, no one can blame you when you don't consider the tradeoffs you make when you use seemingly free platforms. After all, who doesn't love freebies? But there's a very clear motivation for platforms to be free—so that you use them more—and so that you can be mined for more information. It's the reason why information is now more valuable than gold and it's the same reason why companies like Facebook, Google, and Amazon are trillion-dollar companies.

So what makes you and your data so special? The simplest answer is in advertising. The better that advertisers and promoters know you, the more they can sell to you, and relentlessly convince you to buy something you never really needed. But beneath that unsatisfactory reason, lies an even more eerie truth—we are mined and exploited for our data, only to be targeted and controlled in ways we never thought possible. As tinfoil hat conspiracy theorist as that sounds, it's a bitter truth, which is more possible than ever before.

We've seen this before with the Snowden leaks—surveillance of Americans and citizens abroad on a massive global scale, and more recently with Cambridge Analytica and the 2016 Presidential Election of Donald Trump—mass profiling and targeting of Americans to skew their perspectives and ideologies with fake news and other such weapons—all achieved with data collected from Facebook and other data brokers (more on these later). Even if you don't care about politics, think about all the Black Mirror scenarios that can suddenly have the potential of becoming a grim reality—China's 'social credit' system that tracks and punishes it's citizens based on what a Communist Party deems to be right or wrong.

This handbook is curated and written to enlighten you with the information you need to know about your data privacy—what is it, what it means for you, and what you can do about it. This is only scratching the surface of a deep, intricate, and complex world of data privacy. It's highly recommended that you continue to learn, teach, and fight for your data privacy beyond the pages of this handbook.



Firefox Lightbeam is a browser extension that uses interactive visualizations to show you the relationships between third parties and the sites you visit.

Over the course of 8 months, Lightbeam tracked 1,111 websites visited, and recorded 2,007 third party sites that those websites connected and shared data to.

Source: Reddit User Daniellynet

Ch 02.

The What

So what is Data Privacy anyway?

Data privacy relates to how a piece of information—or data—should be handled based on its relative importance. For instance, you likely wouldn't mind sharing your name with a stranger in the process of introducing yourself, but there's other information you wouldn't share, like your bank account information or passwords.

In our current digital age, a lot more information and metrics are collected about us than we realize. Companies today, in a push for innovation, and to maintain an edge over their competitors, analyze, mine, and track virtually everything we do.

These metrics can be as simple as names, emails, dates of birth, or personal as our likes, wants, interests, and desires. Whether we actively realize this or not, chances are your platforms know you better than your friends or even close family members.

The convoluted and obscure nature of data collection and tracking has enabled companies to amass data about everyone without any real oversight. With data now influencing every decision we make, it's now more important than ever to take a strong stance on data privacy.

What do we mean by “Personal Data”?

Right about now, you’re probably thinking that the internet is just one big privacy nightmare. But don’t go off the grid just yet. Personal Data is a pretty vague umbrella term and it helps us to understand what that exactly means for us. Social security numbers, banking information, and health records are amongst the more sensitive data we store online. In contrast, social media posts, search-engine queries, and location data are typically monetized in a higher degree of magnitude that, say, your credit card information isn’t. That isn’t to say that this information itself won’t be revealing. There are other kinds of data collected that also fall into different categories—ones that may surprise you. For example, did you know that there are companies dedicated to analyzing the unique way you tap and interact with your phone? The way you tap, mis-tap, swipe, mis-swipe, or type, are amongst the different metrics that are recorded.

All this data is collected under a wide, open-ended spectrum of consent: Sometimes the data is shared knowingly, and other times (more often that not), the users might not understand they’re giving up anything at all. While sometimes it’s clear that something is being collected, the specifics and minutia of it are often hidden and buried in hard-to-parse terms-of-service agreements, that, let’s face it, no one actually ever reads. There are also cleverly designed Dark UX Patterns (more on this later), that make you want to click and do things that you were intending on. In 2012, Target figured out how to determine whether a woman was pregnant or not, sending them a slew of personalized ads. Where this got especially creepy, however, was when the teenage daughter of a man in Minneapolis was sent coupons for baby clothes and cribs. While the father was enraged at why these coupons were being sent to his daughter, little did he know that she was, in fact, due later that August.

Read: How companies learn your secrets — The New York Times

Let’s look at another example, what happens when someone sends a vial of sliva to 23andme, Ancestry, Natera or FamilyTreeDNA? The person knows they’re sharing their DNA with a genomics company, but they may not ever realize that their information will also be sold to pharmaceutical companies. Many apps also use your location information to show you custom adverts, but they don’t necessarily advertise the fact that certain hedge funds may also buy that location data to analyze which stores you frequent. Any online shopper who’s seen ads directly targeted towards their interests knows they’re being tracked around the web, but fewer people understand that those companies may also be recording not just their clicks, but also their exact mouse movements.

See: Hidden secrets of privacy policies of your favourite platforms — UseGuard

In each of these scenarios, the user received something in return for allowing a corporate entity to monetize their personal data; They got to learn about their genetic ancestry (although, on average, a service like this costs upwards of $100), use a mobile app, or browse the latest footwear trends from the comfort

of their homes. This is the same sort of transaction you make with Facebook and Google. Their core products and services, including Instagram, Messenger, Gmail, and Google Maps, don't cost money. You pay with your personal data, which is used to target you not only with ads but with your ideologies as well.

Play: See how you can be psycho-analyzed with this browser-events based game — ClickClickClick

Source: Wikipedia

What is Collected?

Identity Data

01. Personal Information

Name, Date of Birth, Phone Numbers, Email Addresses, Social Network Handles, Account Infomations, Occupational Information.

02. Demographics

Age and Generation, Gender, Languages, Political Preferences, Parental Status, Maternal Status, Relationship Status, Education Level, Ethnic Affinity.

03. Location

Recently Visited Locations, Interests in visiting Locations, Planned visitations to a location, Postal Address Information.

Quantitative Data

04. Transactional Information

Online and Offline Purchases, Subscriptions, Renewals, Product Abandonments (Not purchased), Product Returns

05. Communication Information

Inbound and Outbound: Communication Dates, Channels, Opens, Clicks, Fowards, etc.

06. Online Activity

Websites Visited, Product Views, Online Registrations, Likes, Tweets, Shares, Followers, Followings.

07. Customer Service Information

Complaints, Complaint Details, Query Details, Transcripts, Recordings, etc.

Descriptive Data

08. Family Details and Life Events

Marital Status, Number of Children, Age of Children, Newly Engaged/Married, Users in new Relationships, Birthdates, Home Purchases, Birth of Children, etc.

09. Lifestyle Details

Properties Owned, Property Values, Property Types, Square Footage of Home, Year Built, Vehicles Owned, Vehicle Value, Pets Owned, etc.

10. Occupational Details

Profession, Education Level, Field of Study, Schools, Industries, Income and Net Worth.

11. Interests

Profile Information, Pages/Posts Liked and Shared, Entertainment Preferences, Shopping Preferences, Food Preferences, Technological Products and Savviness, Travel Requirements (Work Travel) and Preferences (Leisure Travel).

Qualitative Data

12. Attitudinal Information

Customer Service Ratings and Reviews, Product Ratings and Reviews, Likeliness of repurchasing products/services.

13. Opinion Information

Favorite Colors, Foods, Travel Destinations, Wishlists, Bucketlists, etc.

14. Motivational Information

Reasons influencing purchases (personal, gifts, prizes, etc.), Key factors influencing purchases (location, price, quality, availability).

Sample Profile Information

The following Profile Information is taken from a past pre-thesis exploration project, The Data Dossier. Information was requested from different platforms such as Google, Apple, Facebook, Twitter, Instagram, Snapchat, and Microsoft. Compiled below is small sample of information that was included in the 40gb+ archive of files received from these platforms.

Personal Information

Name	Shivam Sinha	/Users/shiv/archive/Google/...
AKA	Shiv Sinha	/Users/shiv/archive/Google/...
DOB	08-11-1997	/Users/shiv/archive/Google/...
Occupation	Designer, Student	/Users/shiv/archive/Google/...

Demographic Information

Age	22	/Users/shiv/archive/Google/...
Gender	Male	/Users/shiv/archive/Google/...
Language	English, Hindi	/Users/shiv/archive/Google/...
Relationship	Single	/Users/shiv/archive/Faceboo...
Education	University Student	/Users/shiv/archive/Instagra...
Ethnic Affinity	Asian, Indian	/Users/shiv/archive/Google/...

Location Information

Current	New York, NY	/Users/shiv/archive/Google/...
Recent	Pittsburg, MA	/Users/shiv/archive/Google/...
	Washington, D.C.	/Users/shiv/archive/Google/...
	Sunnyvale, CA	/Users/shiv/archive/Google/...
	San Fransico, CA	/Users/shiv/archive/Google/...
	Cuptertino, CA	/Users/shiv/archive/Google/...
	Boston, MA	/Users/shiv/archive/Google/...
Past	Singapore	/Users/shiv/archive/Google/...
	New Delhi, India	/Users/shiv/archive/Google/...
	Bangalore, India	/Users/shiv/archive/Google/...
	London, UK	/Users/shiv/archive/Google/...
	Bombay, India	/Users/shiv/archive/Google/...
	Delhi, India	/Users/shiv/archive/Google/...

Lifestyle Details

Car	N/A	/Users/shiv/archive/Google/...
Pets	N/A	/Users/shiv/archive/Google/...
Property	N/A	/Users/shiv/archive/Google/...

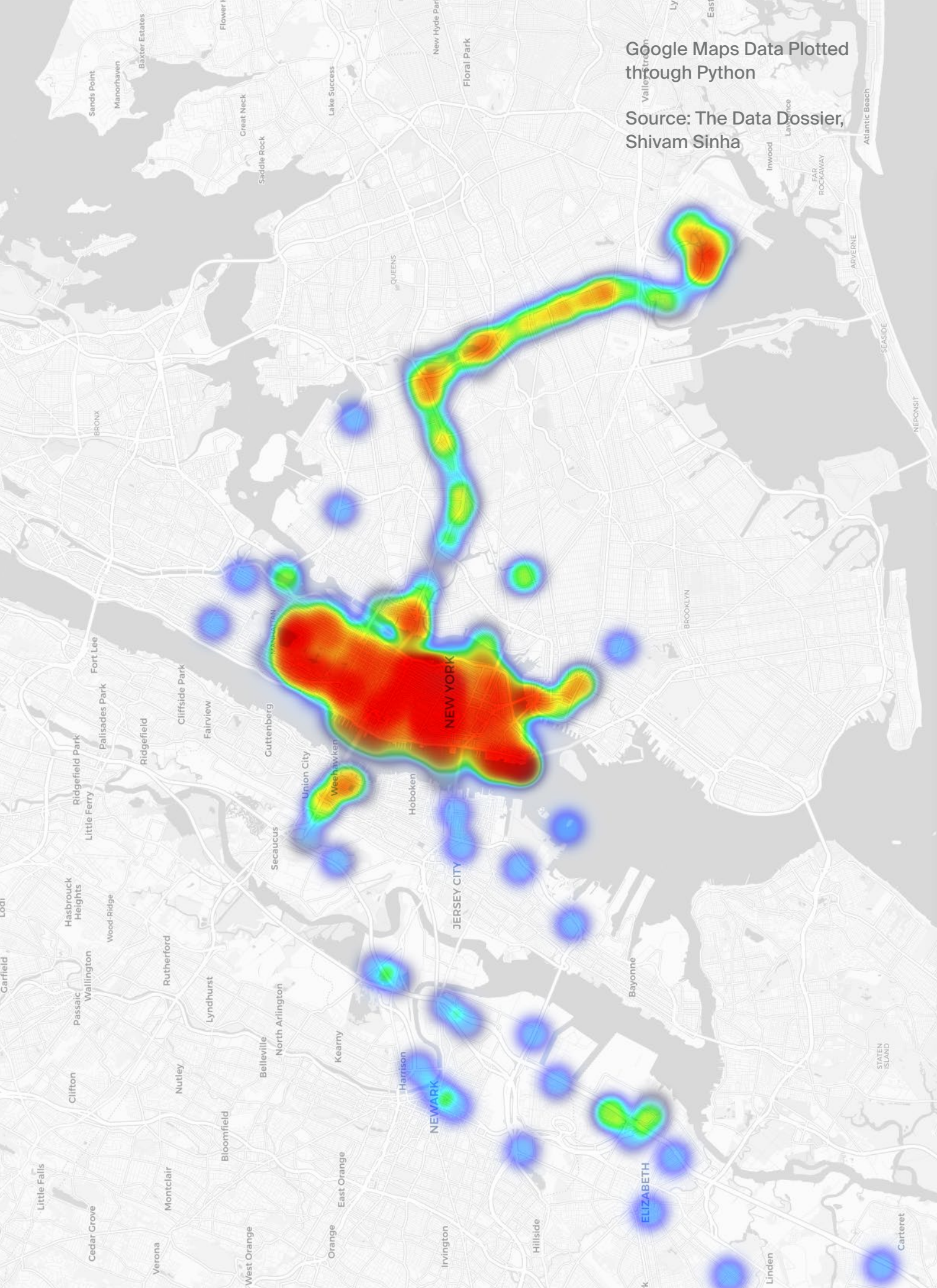
Occupational Information

Profession	Student	/Users/shiv/archive/Faceboo...
Education	Inprogress: BFA	/Users/shiv/archive/Faceboo...
Field of Study	Graphic Design	/Users/shiv/archive/Faceboo...

Read: The Data Dossier — Shivam Sinha (2019)

Interests Information

Movies	007	/Users/shiv/archive/Faceboo...
	2010 MU F.C.	/Users/shiv/archive/Faceboo...
	9GAG	/Users/shiv/archive/Faceboo...
	AIGA	/Users/shiv/archive/Faceboo...
	Action Movies	/Users/shiv/archive/Faceboo...
	Adam Diver	/Users/shiv/archive/Faceboo...
	Adult Swim	/Users/shiv/archive/Faceboo...
	BBC One	/Users/shiv/archive/Faceboo...
	Black Comedy	/Users/shiv/archive/Faceboo...
	Buzzfeed	/Users/shiv/archive/Faceboo...
	Cartoon Network	/Users/shiv/archive/Faceboo...
	DC vs. Marvel	/Users/shiv/archive/Faceboo...
	Everlane	/Users/shiv/archive/Faceboo...
	Fantasy Movies	/Users/shiv/archive/Faceboo...
	Fine-Art	/Users/shiv/archive/Faceboo...
	Game of Thrones	/Users/shiv/archive/Faceboo...
	House of Cards	/Users/shiv/archive/Faceboo...
	Hulu	/Users/shiv/archive/Faceboo...
	James Bond	/Users/shiv/archive/Faceboo...
	Loading Artist	/Users/shiv/archive/Faceboo...
	LucasFilms	/Users/shiv/archive/Faceboo...
	MTV	/Users/shiv/archive/Faceboo...
	Mark Hamill	/Users/shiv/archive/Faceboo...
	MCU	/Users/shiv/archive/Faceboo...
	Netflix	/Users/shiv/archive/Faceboo...
	Paper Bag	/Users/shiv/archive/Faceboo...
Music	Alan Silvestri	/Users/shiv/archive/Faceboo...
	Hans Zimmer	/Users/shiv/archive/Faceboo...
	Electronic	/Users/shiv/archive/Faceboo...
	New York Jazz	/Users/shiv/archive/Faceboo...
	Indie Electronic	/Users/shiv/archive/Faceboo...
	Coldplay	/Users/shiv/archive/Faceboo...
	Frank Ocean	/Users/shiv/archive/Faceboo...
	Headphones	/Users/shiv/archive/Faceboo...
	LCD Soundsystem	/Users/shiv/archive/Faceboo...
	Instrumental	/Users/shiv/archive/Faceboo...
Tech/Games	Apple	/Users/shiv/archive/Faceboo...
	Nvidia	/Users/shiv/archive/Faceboo...
	Call of Duty	/Users/shiv/archive/Faceboo...
	Microsoft	/Users/shiv/archive/Faceboo...
	Google	/Users/shiv/archive/Faceboo...
	Gadgets/Tech	/Users/shiv/archive/Faceboo...
	Samsung	/Users/shiv/archive/Faceboo...
	Wired (Magazine)	/Users/shiv/archive/Faceboo...



Google Maps Data Plotted through Python

Source: The Data Dossier, Shivam Sinha

Ch 03.

The Why

I've got nothing to hide. Why should I care?

Your information has value. Companies like Facebook and Google allow you to upload unlimited data to their servers, for free. What's their business model? How do they make so much money? They sell your info to advertising companies and data brokers. But they never asked you if you wanted to sell your information. If someone asked you, in person, 100 questions about your personal life with the intent of selling the information, would you answer them? Probably not, right? But you let this happen every time you use a service that makes money selling your info.

Other than value, there are two sets of reasons to care about your privacy even if you've got nothing to hide—ideological reasons and practical reasons. Ideologically, privacy is a right that we haven't always had. Just like the right to freedom of speech, generations before ours have fought for our right to privacy as a human right.

Having nothing to hide is not true nor realistic. Don't confuse privacy with secrecy. Everyone knows what you do in the bathroom, yet you still close the door. That's because you want privacy, not secrecy. Just like you have a passcode for your phone, and passwords for your email because you don't want people reading your personal messages.

Practically, especially, information in the wrong hands becomes dangerous. You might be okay with governments or security agencies having your private information. You might even trust Google or Facebook with all of your information. But what if these trusted platforms get hacked and your information falls in the wrong hands? What, or who would your information make you vulnerable to? You also can't predict the future. Right now you may not have a lot to risk, but what about 30 or 40 years from now? If Sony's hacking has told us anything, is that your private information has an impact on your life. Amy Pascal, co-chairman of the company, lost her job because of the company's reckless security.

Your private life out of context becomes a weapon. In "secure chats" or closed doors with friends or colleagues, we've all made comments or said comments that we regret, or might be misinterpreted by others out of context. In fact, our behavior changes depending on the people we're with. Someone could easily find something offensive you said in a group chat that you have with your closest friends. Because they're your friends and it was a joke or a sarcastic remark. But take it out of context and it is no longer a joke.

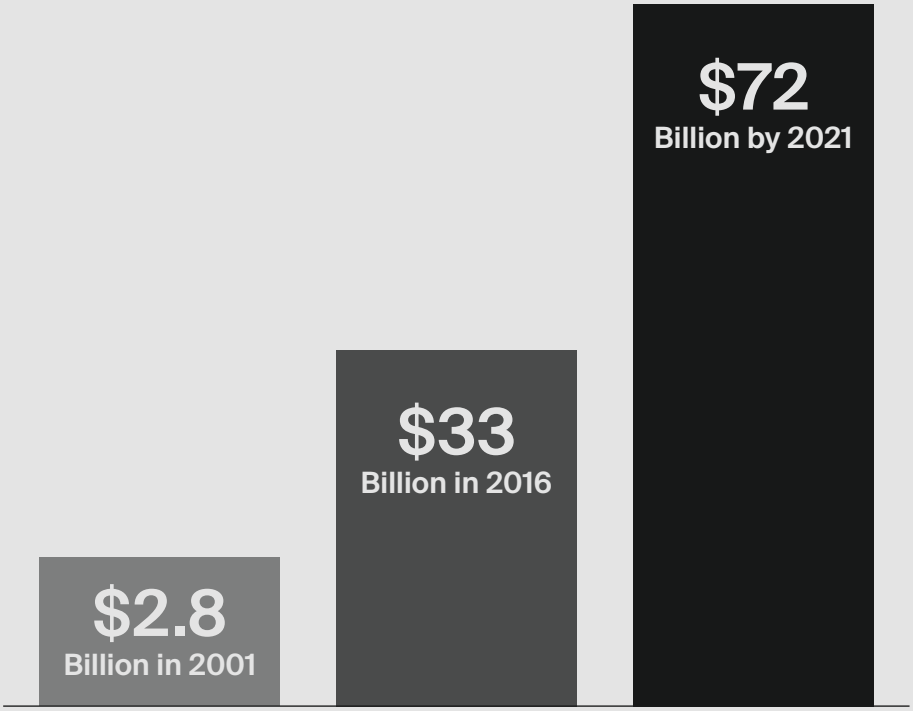
With the 2020 COVID-19 pandemic forcing people to stay home, work from home, and now spend more time on their digital devices than ever before, it becomes imperative to talk about why privacy matters. As schools and businesses transitioned to conduct classes and meetings on the popular video conferencing app, Zoom, little did they know that their data was also being

Read: How Zoom was selling data to Facebook, even if you weren't a Facebook user

shared with Facebook, regardless of whether they were Facebook users or not. When caught publicly, Zoom quickly reversed the code to stop sharing data with Facebook. Yet another bug in the app's code also made it possible for what is now referenced to as "Zoombombing"—trolls of the internet jumping into public Zoom calls and using the platform's screen-sharing feature to project graphic content to unwitting conference participants, forcing hosts to shut down their events. As we increasingly become more and more dependent on these technologies, we must ask ourselves about the tradeoffs we're making by using these services. We must demand oversight change on an industry-wide level.

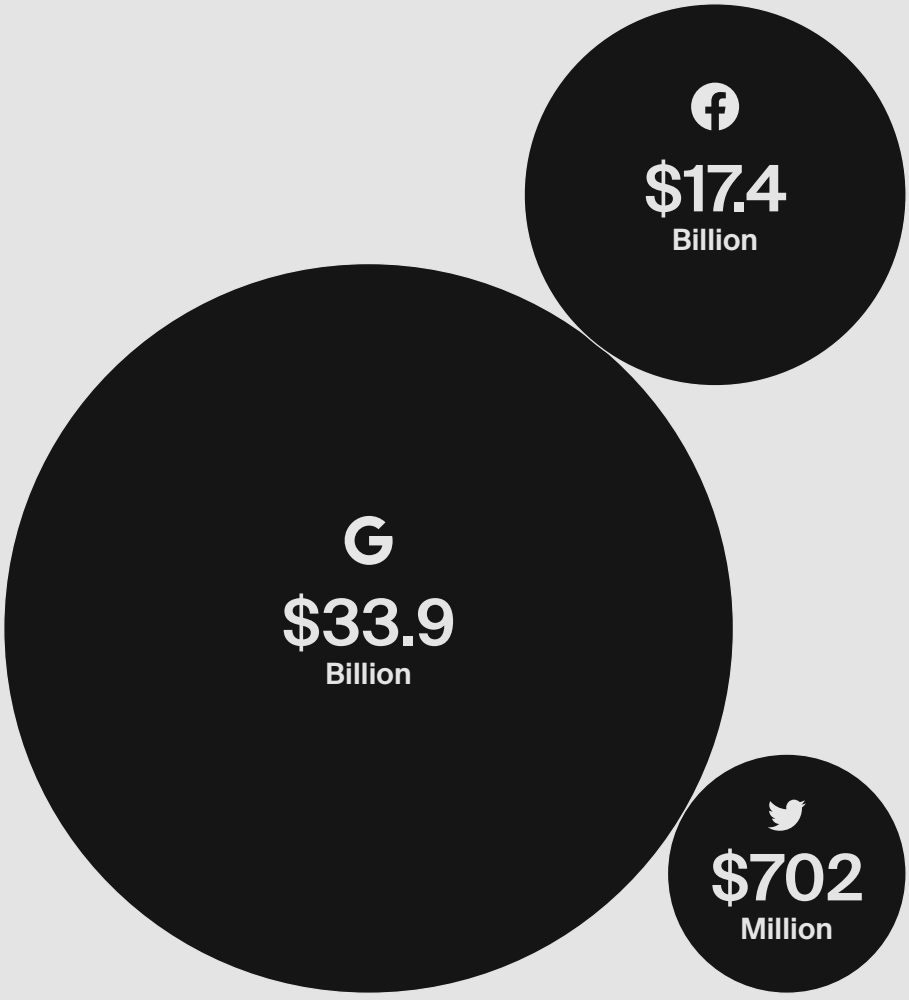
Source: Via Twitter user @exitpost

The Numbers — Targeted Ads



Total Spending on Ads

Watch: Do Not Track — S01E02: Breaking Ad



Social Media Revenue (Q3 2019)

Source: Pew Research Center, BigCommerce, Internet World Stats, Mobile Ecosystem Forum 2018, Express VPN. Via Privacy Monitor.

Ch 04.

The How

Humans have used devices to collect data about the world for many years now. Greek scientists used an intricate gear system called the Antikythera mechanism, to trace astrological patterns as far back as 150 BC. Two thousand years later, Herman Hollerith invented the tabulating machine, a device that helped process data from the 1980 United States Census. Hollerith founded the company that later merged to become what is now IBM.

By the 1960s, the US government was using powerful machines to store and compute information on nearly every American. Companies also started using these machines to analyze information about consumer purchasing habits. With no oversight to what companies could collect, worries over invasive surveillance soon emerged, especially after Vance Packard's 1964 book, The Nakes Society, argued that technological innovation was causing the unprecedented depletion of privacy. Soon after, President Lyndon Johnson's administration tried to merge hundreds of federal databases into one centralized National Data Bank. Congress, concerned about the possibility of invasive surveillance, pushed back on that idea and created the Invasion of Privacy subcommittee. The National Data Bank was never realized, and to ensure the protection of personal data, Congress passed a series of laws including the Fair Credit Reporting Act of 1970 and the Privacy Act of 1974. While the regulations outlined the transparency of data collection, it did nothing to prevent the government and corporations from collecting the information to begin with.

By the end of the 1960s, some scholars, including MIT political scientist Ithiel de Sola Pool, predicted that new digital technologies would continue to facilitate even more invasive personal data collection. By the time everyone was online in the mid-1990s, that reality was beginning to take shape. The Lotus Corporation and the credit bureau Equifac teamed up to create Lotus MarketPlace: a CD-ROM marketing product that boasted to contain names, income ranges, addresses and other such information about more than 120 million Americans. The retaliation from privacy advocated ultimately cancelled the product before it was ever publicly released. Soon after, ads began to pop-up around the web. While in the early stages of this time, advertisements remained anonymous, attempts were soon made to de-anonymize ads. In 1999, the digital ad giant DoubleClick, ignited a privacy scandal when it tried to merge it's ad data with the enormous data broker, Abacus Direct.

DoubleClick was eventually sold at a loss in 2006, when privacy groups petitioned the Federal Trade Commission (FTC), arguing that the practice would amount to unlawful tracking of Americans. As a result, the Network Advertising Initiative was created. A trade group that developed the standards for online advertising, including requiring companies to notify

users when their personal data was being collected. Eventually, though, privacy advocates lost the battle when Google bought DoubleClick in 2016, and amended it's privacy policy to permit personally-identifiable data. Today, companies like Google and Facebook can track and target ads based on your name and information. Exactly what people feared when DoubleClick would do almost 20 years ago.

How is your information collected?

As we can see, in the past, there has been little to no oversight in what can be recorded, stored, or used about you and your personal lives. While in the past, data brokers and platforms have been limited to rather mundane and straight-forward ways of tracking you, modern technologies have streamlined, and supercharged the way platforms and data brokers can now mine us for our data.

Here are a few components about your browser, both desktop and mobile, that are used to track you on your daily online adventures.

Traditional Cookies

Facebook, Google, and other companies use these extremely popular cross-site trackers to follow users from website to website. They work by depositing a piece of code into the web browser, which users then unwittingly carry with them as they surf the infinite web.

Super Cookies

These are similar to traditional cookies, in that they contain just about any information including browsing history, authentication details or ad-targeting data, however, they are designed to be permanently stored on the user's computer. They were most famously used by Verizon, which had to pay a $1.35 million fine to the FCC as a result of the practice.

Fingerprinting

These cross-site trackers follow users by creating a unique profile of their device. They collect things like the person's IP address, their screen resolution, what type of computer they have, and even what type of fonts they have installed. This enables them to form a unique identity of you based off of these data points.

Identity Trackers

Instead of using a cookie, these rare trackers follow people using personally identifiable information, such as their email address. They collect this data by hiding on login pages where people enter their credentials.

Session Cookies

Some trackers are good! These helpful same-site scripts keep you logged in to websites and remember what's in your shopping cart—often even if you close your browser window. However, these can be exploited by websites with ill intent.

Session replay Scripts

Some same-site scripts can be incredibly invasive. These record everything you do on a website, such as which products you clicked on and sometimes even the password you entered.

Social Media Trackers

Logging into websites using your Google or Facebook account can often be a handy and streamlined way of creating accounts, but you're also duped into sharing way more information that you need to, not just with that website, but also the platform you used to log in. This also applies to embedded posts, tweets, and youtube videos that you see in articles across the internet.

Email Trackers

For popular email services like Gmail and Yahoo, your emails are also scanned for keywords, interests, and topics you like—helping advertisers sell to you better. But that's not all, newsletters you receive are also ways in which you are tracked and profiled for the services and apps you use.

Keep in mind that this is just your web browser, using apps and other plugins can afford the platforms other backdoors to keep tabs on you. Here are a few ways in which using Apps and Plugins can allow for more avenues in tracking you:

Read: How The New York Times was able to track Donald Trump and members of the Secret Service through publicly available GPS data.

Location Data

This one is rather straight-forward: Apps can capture your GPS data and send them to their respective servers for storage and analysis. Google Maps, for example, sends upwards of 300 location pings daily on an Android phone.

Bluetooth Scanning Data

Apart from your location data, if you have your Bluetooth enabled at all times, your device will intermittently capture other Bluetooth devices available to connect to. These devices can share their names, device types, and other identifying information that can be used to fingerprint you further.

WiFi Scanning Data

Much like Bluetooth scanning, your phone and laptop will also scan for available public networks available to connect to. This information can contain the network name, location, IP addresses that can be used to pinpoint your location. So even if you have your location services disabled, ill-intent apps can still triangulate

your estimated position through these scans.

Device Identifiers

Your device, by itself, can also reveal a lot about you: An app can request the name, make, model, serial number, network carrier information, and even the color of your phone, to create a unique fingerprint of you.

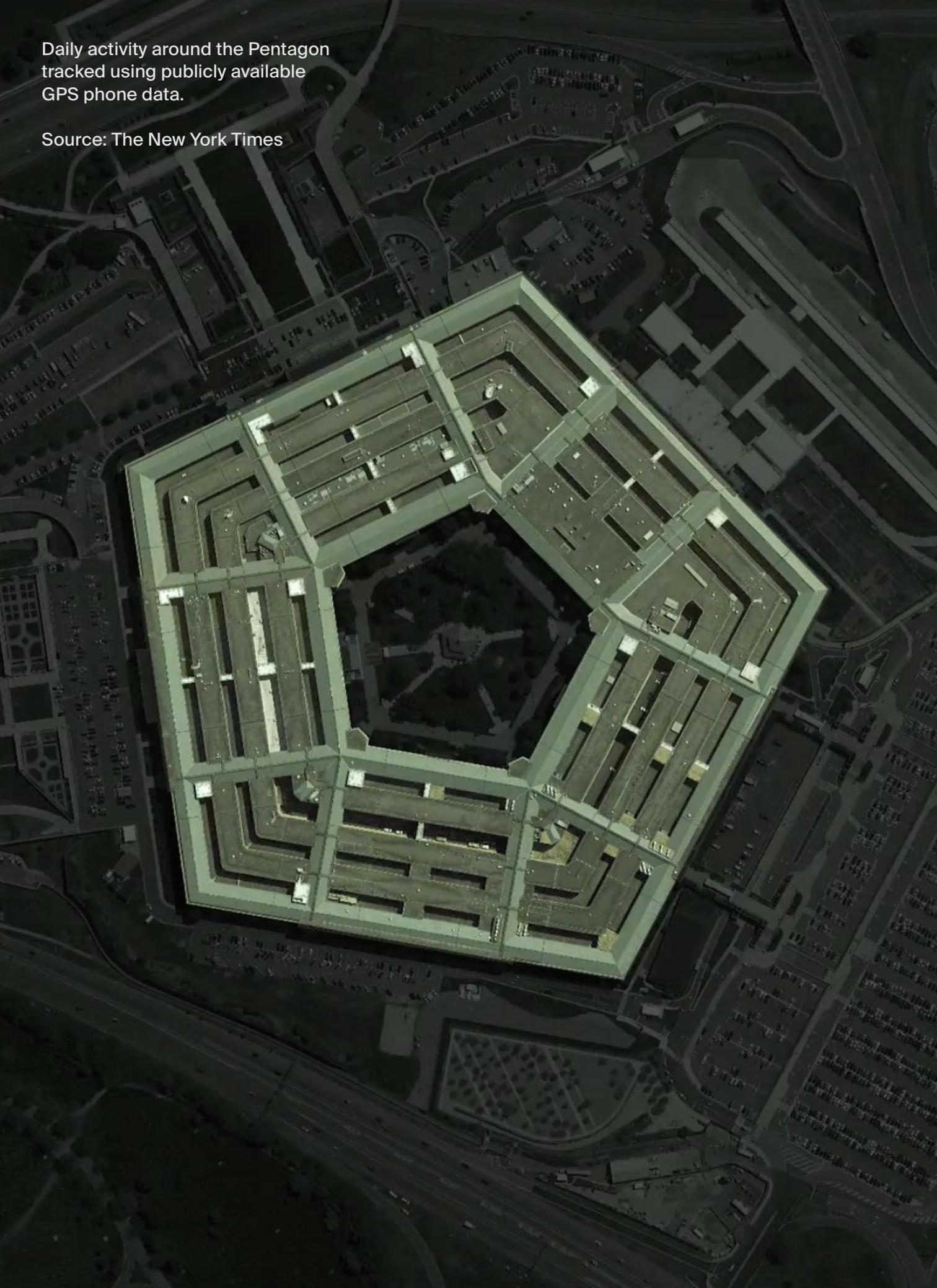
Device Sensor Data

Perhaps the scariest of the list is your device sensor information. Modern devices, like the iPhone 11 Pro, contain a vast array of advanced sensors that can detect your physical state (i.e. sitting, lying, walking), your location, your ambient lighting conditions, and ambient sound information. In some cases, apps were able to get personal health information from your device, which can include information like age, weight, height, and even heart rate data.

Play: See how this unconventional game, winner of Apple's Design Award, makes use of your device's sensors to create innovative puzzles.

While at times, these kinds of methods are out of the user's control, there are very many cases where the user is directly responsible for sharing data, even if they didn't want to. This is where Dark UX Patterns come in. User experience (UX) in general, is a field that's dedicated to making the user's life simpler and efficient in what they are trying to achieve. Oftentimes, UX design is so effective, that users are able to achieve their goals in a few simple taps. This is where Dark UX Patterns prey on their users—using muscle memory and time as a tool, Dark UX Patterns are cleverly designed experiences that make you do something you didn't intend on. Sometimes, it can be as simple as clicking something, other times, it can be as extreme as sharing your entire contacts list. When you use websites and apps, you don't read every word on every page - you skim read and make assumptions. If a company wants to trick you into doing something, they can take advantage of this by making a page look like it is saying one thing when it is in fact saying another. So the next time you're gliding through a website, make sure to pause, and make sure you fully understand what you're clicking on or agreeing to.

Read: More about Dark UX Patterns.



Daily activity around the Pentagon tracked using publicly available GPS phone data.

Source: The New York Times

The future of Data Collection:

Data collection in our current technical landscape has primarily been done through screens when people use computers and smartphones. However, the coming years will bring new data-guzzling devices like wearable health tech, sensor-embedded clothing, AR glasses, smart lights, home automation tech, and so much more. We've already seen a glimpse of these products through products like smart speakers and the several scandals they've already been in. But even for those who refrain from using these devices, will likely have their data gathered, with the adoption of facial recognition-enabled cameras across the most urbanized cities. In so many ways, this future has already begun—Taylor Swift fans have had their faces collected, and Amazon Echoes and Google Homes around the world have been listening in on millions of homes.

Watch: Netflix's Black Mirror — S01E03: The Entire History of You

We haven't yet decided, though, how should we navigate this new data-harvesting landscape. Afterall, we can't expect laws from nearly 50 years ago to keep up with the rapidly changing landscape of the tech industry. Do we really want health insurance companies tracking our eating and shopping habits? Should colleges be permitted to digitally track their applicants through their social media? It is now more imperative than ever, to start asking these questions.

Perhaps, as scientists continue to push the boundaries of what's possible with artificial intelligence, we will also need to learn to make sense of the personal data that isn't even real, but fabricated by algorithms that other machine learning algorithms can train on. With the rise of the so-called deepfake technologies, propagandists and hoaxers can now leverage social media photos to recreate videos that depict events that never happened. AI can now create millions of synthetic faces that don't belong to anyone, altering the definition of identity-theft. This fraudulent data could further blur the line between what's real and what's fake on social media. Imagine trying to discern whether your Tinder match or the person you just followed on Instagram is actually real or not.

Watch: Her (2013), directed by Spike Jonze, starring Joaquin Phoenix and Scarlett Johansson

Regardless of whether data is fabricated by computers or created by real people, a big concern yet remains on how this data will be analyzed. It's important to understand that not only the information we collect matters, but what inferences and predictions we make from that data that matters equally, if not more. Our personal data is already being used by algorithms to make important decisions like whether someone should maintain their health care benefits, or if someone should be released on bail. These decisions can easily be biased, and researchers at companies like Google are now working on making algorithms and the datasets that are used to train them, more transparent and fair.

Tech companies are now also beginning to acknowledge that data collection needs to be regulated. While Microsoft has called

for the federal regulation of facial recognition technology, Apple's CEO Tim Cook has called on the FTC to establish a clearinghouse where all data brokers will need to register. Some companies and researchers argue, however, that it's never going to be enough for the government to simply protect personal data; Consumers will need to take ownership of their own data, and be compensated for when it's used. Social media like Minds and Steemit, as well as the privacy focussed browser, Brave, have already experimented with rewarding users with cryptocurrency in exchange for some pre-vetted ads. Other companies will pay you in exchange for sharing your data, for example, the app Sweatcoin tracks your steps, and offers free products through spending the accumulated in-app currency. There are, however, doubts about people taking ownership back as well, as it won't solve every privacy issue posed by the collection of personal data. Instead, it might be more practical to reframe the problem—perhaps less collection should be permitted in the first place and businesses should be encouraged to move away from the targeted-advertising business model altogether.

Read: This Instagram influencer, Lil Miquela, isn't actually real.

Source: Via Lil Miquela on Instagram

Can data collection help train Artificial Intelligence to cure lonliness and help us find true love? If so, would we want to?

Source: *Her (2013)*

Ch 05.

The Who

Who has my data?

The exchange you make between the services you use for free with your personal data, may or may not be worth it to you, but there's another, seedier breed of businesses out there that amasses, analyzes, and sells your information without giving you anything back at all: Data Brokers. These companies compile information from various public sources like property records, marriage licenses, and court cases. They may also buy and gather information like your medical records, browsing history, location data, social media connections, and online purchases. Depending on where you live and who you are, data brokers might even purchase information from the Department of Motor Vehicles. Don't drive? Retail stores can sell your information to data brokers too.

While the information Data Brokers collect on you might be outdated or inaccurate, it can still be incredibly valuable to companies, marketers, investors, and other individuals. In fact, American companies alone have been estimated to have spent over $19 billion in 2018 acquiring and processing consumer data, according to the Interactive Advertising Bureau. Surveillance data and tools can also be maliciously misused by individuals such as stalkers or in domestic abuse situations. Doxxing, the practice of publicly releasing someone's private information without their consent, often to damage their reputations, is usually possible because of data brokers. While deleting your online accounts with big platforms can be easy, removing your information from these data brokers can be extremely time-consuming, and nearly impossible.

Amassing and selling your data for profit like this is (oddly) perfectly legal. While states like California and Vermont have recently moved to put more restrictions in place for data brokers, they still largely remain unregulated. The Fair Credit Reporting Act (FCRA) dictates how data collected for credit, employment, and insurance may be used, but some data brokers have been caught breaking that law. In 2012, the "personal lookup" site Spokeo settled with the FTC for $800,000 for advertising its services for purposes like job background checks. Plus, data brokers who market themselves as digital phone books, don't have to abide by these regulations in the first place.

There are also very few laws that govern how social media companies may collect data about their users. In the US, no modern federal policy exists to regulate data collection, and the government can legally request digital data held by companies without a warrant in many circumstances.

Mark Zuckerberg speaks to press and advertising partners in 2007. Two weeks after announcing its new marketing program, the company faced complaints from users surprised to find information about their online purchases added to their personal news feeds.

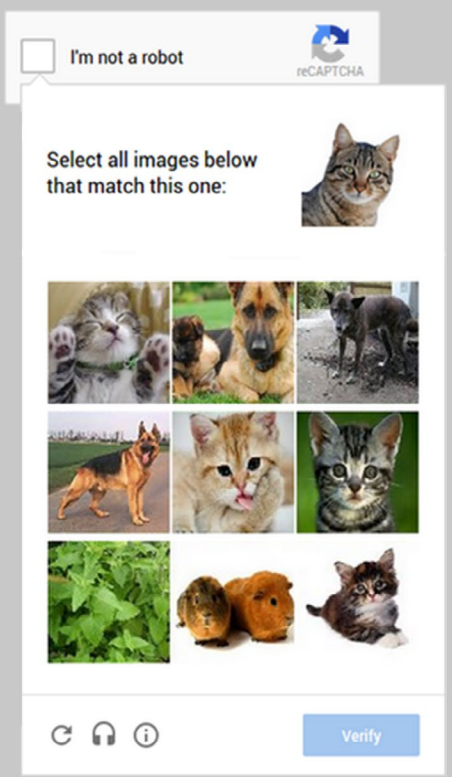
Ch 06.

Ending Notes

The Silver Lining:

The bright side of all this is, the information you share online also contributes to the global store of useful knowledge—researchers from a number of academic disciplines study social media and other user-generated data to learn more about how we as a humanity functions. Author Seth Stephens-Davidowitz, in his book, Everybody Lies: Big Data, New Data, and What the Internet Can Tell Us About Who We Really Are, argues that people are often more honest with sites like Google than they are in real life and traditional surveys. For example, he claims, fewer than 20% of people admit that they watch porn, yet there are more Google searches for “porn” than “weather”.

Our personal data is also used by artificial intelligence researchers to train their automated models. Everyday, users around the world upload billions of photos, videos, gifs, texts, and audio clips to social media websites. This media is then fed to machine learning algorithms, so that they can learn to “see” and discern different parts of a photograph. Remember those annoying CAPTCHAs (Completely Automated Public Turing Test to tell Computers and Humans Apart) around the internet? The ones that ask you to prove that you are human? Yup, you guessed it, it’s actually using you to make itself smarter. So the next time you upload a selfie, you might actually make an AI smarter.



Source: Google reCAPTCHA

Further Reading and Resources:

“Data & Society.” Data & Society, https://www.datasociety.net/.	
“EFF Action Center.” EFF Action Center, Electronic Frontier Foundation, https://act.eff.org/.	
“Ethical Alternatives & Resources.” Ethical, https://ethical.net/resources/.	
“Find out If You've Been Part of a Data Breach.” Firefox Monitor, Firefox, https://monitor.firefox.com/security-tips.	
“How Is Your Website Impacting the Planet?” Website Carbon Calculator. https://www.websitecarbon.com/.	
“My Browser Fingerprint.” AmIUnique, https://www.amiunique.org/fp.	
“Prediction API.” Apply Magic Sauce, University of Cambridge, https://applymagicsauce.com/demo.	
“The Privacy Project.” The New York Times, The New York Times, 11 Apr. 2019.	
Gartenberg, Chaim. “Why Amazon Is Tracking Every Time You Tap Your Kindle.” The Verge, 31 Jan. 2020,	
Hunt, Troy. “Check If You Have an Account That Has Been Compromised in a Data Breach.” HaveIBeenPwned?	
Odrozek, Kasia. “The Good, the Bad and the Ugly Sides of Data Tracking.” Internet Health Report 2018, Mozilla, 11 Apr. 2018.	
Shulevitz, Story by Judith. “Alexa’s Most Dangerous Feature Can’t Be Undone.” The Atlantic, Atlantic Media Company, 7 Nov. 2018.	
Tech, Tactical. “The Data Detox Kit: Learn the Essentials.” Data Detox Kit, https://datadetoxkit.org/en/home.	

References:

"Data Protection Guide." Privacy International | Data Protection Guide, privacyinternational.org/sites/default/files/2018-09/Data%20Protection%20COMPLETE.pdf.

"Encryption Against Global Mass Surveillance." PrivacyTools, www.privacytools.io/.

"The Modern Web Is Becoming an Unusable, User-Hostile Wasteland • Abid Omar." Abid Omar, 20 Dec. 2019, omarabid.com/the-modern-web.

"The Privacy Project." The New York Times, The New York Times, 11 Apr. 2019, Accessed March 2020, www.nytimes.com/interactive/2019/opinion/internet-privacy-project.html.

Anna Fielder, 'Why we need collective redress for data protection', Privacy International Medium, 9 January 2018, https://medium.com/@privacyint/why-we-need-collective-redress-fordata-protection-863c6640689c.

Clover, Juli. "FCC: Wireless Carriers Violated Federal Law by Sharing Consumer Location Data." MacRumors, MacRumors, 31 Jan. 2020, www.macrumors.com/2020/01/31/fcc-carriers-illegal-location-data-sharing/.

Coleman, Kevin. "Awesome Privacy." GitHub, 22 June 2019, github.com/KevinColemanInc/awesome-privacy.

Gartenberg, Chaim. "Why Amazon Is Tracking Every Time You Tap Your Kindle." The Verge, 31 Jan. 2020, www.theverge.com/2020/1/31/21117217/amazon-kindle-tracking-page-turn-taps-e-reader-privacy-policy-security-whispersync.

Jack, Caroline. Data Society Annual Report. Microsoft, 2018, Data Society Annual Report, datasociety.net/annualreport/wp-content/uploads/Data_Society_Annual_Report_2017-2018_SP.pdf.

Janc, Artur, and Michal Zalewski. "Technical Analysis of Client Identification Mechanisms - The Chromium Projects." Chromium Security, Google Chrome, sites.google.com/a/chromium.org/dev/Home/chromium-security/client-identification-mechanisms#TOC-Machine-specific-characteristics.

Jeremy B White, 'Cambridge Analytica ordered to turn over man's data or face prosecution', The Independent, 5 May 2018, https://www.independent.co.uk/news/uk/home-news/cambridge-analytica-ordered-ico-personal-data-davidcarroll-a8338156.html

Klosowsk, Thorin. "How to Protect Your Digital Privacy." The New York Times, The New York Times, www.nytimes.com/guides/privacy-project/how-to-protect-your-digital-privacy.

Kwet, Michael. "In Stores, Secret Bluetooth Surveillance Tracks Your Every Move." The New York Times, The New York Times, 14 June 2019, www.nytimes.com/interactive/2019/06/14/opinion/bluetooth-wireless-tracking-privacy.html.

Odrozek, Kasia. “The Good, the Bad and the Ugly Sides of Data Tracking.” Internet Health Report 2018, Mozilla, 11 Apr. 2018, internethealthreport.org/2018/the-good-the-bad-and-the-ugly-sides-of-data-tracking/.

Pasquale, Frank. “7 Ways Data Currently Being Collected About You Could Hurt Your Career or Personal Life.” HuffPost, HuffPost, 7 Dec. 2017, www.huffpost.com/entry/data-collected-hurt-career-personal_b_6110682?guccounter=1.

Privacy International, ‘Data is power: Towards additional guidance on profiling and automated decision-making in the GDPR’, 2017, https://www.privacyinternational.org/report/1718/data-power-profiling-and-automated-decisionmaking-gdpr

Privacy International, How Do Data Companies Get our Data?, 25 May 2018, https://privacyinternational.org/feature/2048/how-do-datacompanies-get-our-data

Privacy International, Uncovering the Hidden Data Ecosystem, https://privacyinternational.org/campaigns/uncovering-hidden-data-ecosystem

Rameerez, Javi. “UseGuard.” Discovery the Hidden Secrets in Privacy Policies, 2019, useguard.com/products.

Schmidt, Douglas C. Google Data Collection. Digital Content Next, 2018, Google Data Collection, digitalcontentnext.org/wp-content/uploads/2018/08/DCN-Google-Data-Collection-Paper.pdf.

Upian. Do Not Track. Do Not Track, National Film Board of Canada, 2019, donottrack-doc.com/en/episodes/.

Colophon:

This handbook was designed and made by Shivam Sinha, through the assistance of my professor, Joe Marianek, at the Parsons School of Design. It was type set in Suisse Intl. It was designed in Adobe InDesign CC 2020 with all images edited in Adobe Photoshop CC 2020 or created in Adobe Illustrator CC 2020. This booklet was printed on 24th April 2020.

This interview booklet is printed on the Lulu Expresses’s color printers, in tabloid sized, on bright white, 80LB Felt Paper.

All text used in this book are either original, quoted, or paraphrased from their appropriate references.

All images were collected from their respective sources, with some image modified in Adobe Photoshop CC 2020 to better work within the context of this book.

All placeholder text, QR codes, or misc elements were generated in Adobe InDesign CC 2020.

Special thanks to Arani Halder, Eli Lederberg, Esra Gumrukculer, Sanjay Sinha, Simon Sciacovelli, and Sophia Marinelli for proof-reading and feedback.

Get Actionable Steps:
data-aeternum.com