*****Data Privacy In The Age of Internet and Social Media*

**The Surprising Failure Of Anonymization**

In today’s landscape it seems inevitable that the companies who supply our on-line experience are going to collect data about us, about how we use their products for the purported benefit to us the users of an improved digital experience. Tech companies have thus far relied heavily on promises of anonymization to assure their customers that their collected personal data was safe. Several relatively simple experiments have shown that re-identification of anonymized data is frighteningly easy[[1]](#footnote-1). "Aggregate and anonymous" isn't a credible defense, especially with advertisers and government knocking on the doors of these developers, begging for a peek at that "anonymous, aggregate" data.

Law professor Paul Ohm, an outspoken advocate for data privacy who wrote *The Surprising Failure Of Anonymization* said, "Reidentification science disrupts the privacy policy landscape by undermining the faith that we have placed in anonymization… This is no small faith, for technologists rely on it to justify sharing data indiscriminately and storing data perpetually, all while promising their users (and the world) that they are protecting privacy. Advances in reidentification expose these promises as too often illusory."

Ohmn’s Law - "Data can either be useful or perfectly anonymous, but never both." This is the pressure tech companies face to not fully anonymize the data they collect. It becomes far less useful to them in that form. Anyone involved in tech knows there is no such thing as a perfectly safe database which means that this identifiable data is a risk for us.

**Why Should You Be Concerned About Data Privacy?**

You’ve done nothing wrong. You’ve got nothing to hide. We are coming realize that such beliefs are Pollyannaish. The ACLU provides these six reasons[[2]](#footnote-2) to be concerned about data privacy:

1. **Some people do have something to hide, but not something that the government ought to gain the power to reveal.** People hide many things from even their closest friends and family: the fact that they are gay, the fact that they are sick, the fact that they are pregnant, the fact that they are in love with someone else. Though your private life may be especially straightforward, that should not lead you to support policies that would intrude on the more complicated lives of others. There's a reason we call it *private* life.
2. **You may not have anything to hide, but the government may *think* you do.** One word: errors. If we allow the government to start looking over our shoulders *just in case* we might be involved in wrongdoing-mistakes will be made. You may not think you have anything to hide, but still might end up in the crosshairs of a government investigation, or entered into some government database, or worse. The experience with terrorist watch lists over the past 10 years has shown that the government is highly prone to errors, and tends to be sloppily overinclusive in those it decides to flag as possibly dangerous.
3. **Are you *sure* you have nothing to hide?** As I said in this 2006 piece, there are a lot of laws on the books-a lot of *very complicated* laws on the books-and prosecutors and the police have a lot of discretion to interpret those laws. And if they decide to declare you public enemy #1, and they have the ability to go through your life with a fine-tooth comb because your privacy has been destroyed, they will find something you'll wish you could hide. Why might the government go after you? The answers can involve muddy combinations of things such as abuse of power, mindless bureaucratic prosecutorial careerism, and political retaliation. On this point a quotation attributed to Cardinal Richelieu is often invoked: "Give me six lines written by the hand of the most honest man, and I'll find something in them to hang him by."
4. **Everybody hides many things even though they're not wrong.** The ultimate example is the fact that most people don't want to be seen naked in public. Nudity also makes a good metaphor for a whole category of privacy concerns: just because we want to keep things private doesn't mean we've done anything wrong. And, it can be hard to give rational reasons why we feel that way-even those of us who feel most comfortable with our bodies. True, some people may be perfectly happy posting nude pictures of themselves online, but other people do not like to show even a bare ankle-and they should have that right. In the same way, there may not be anything particularly embarrassing about other details of our lives-but they are our details. The list of all the groceries you have purchased in the past year may contain nothing damaging, but you might not want a stranger looking over that either, because of that same difficult-to-articulate feeling that it would just be, somehow, *invasive*, and *none of their damned business*. As Bruce Schneier aptly sums it up, "we do nothing wrong when we sing in the shower."
5. **You may not care about hiding it, but you may still be discriminated against because of it.** As I discussed recently in this post about data mining, people are often denied benefits or given worse deals because some company decides that some behavior-entirely innocent and legal-might suggest you are a poor risk. For example, credit card companies sometimes lower a customer's credit limit based on the repayment history of the *other customers* of stores where a person shops.
6. **Privacy is about much broader values than just "hiding things."** Although many people will want more specific answers to the question such as the above, ultimately the fullest retort to the "nothing to hide" impulse is a richer philosophical defense of privacy that articulates its importance to human life-the human need for a refuge from the eye of the community, and from the self-monitoring that living with others entails; the need for space in which to play and to try out new ideas, identities, and behaviors, without lasting consequences; and the importance of maintaining the balance of power between individuals and the state.

And one last one. **Social Credit Ratings**. It is hard to imagine that the United States could ever get here, but the tech sector has repeatedly shown a cavalier attitude when it comes to respecting privacy when there is money to be made. The Chinese Social Credit System resembles and American credit score. In one province, names of residents with the highest scores are displayed with pride outside city hall, and the public library. But a low score can lead to bans from travel, certain schools, hotels, government positions and even dating apps. While we might agree with the system’s rewards for good behaviors (e.g. donating to a blood bank or charity, performing a heroic act etc.) it would be folly not to recognize that such a system could doom some people by limiting their access to opportunities to generate positive credits due to low education, an isolated social network, or untrustworthiness from having a low score to begin with. Xi Jinping has described the system’s foundation “Once untrustworthy, always restricted.”

**Ways to Limit Your Exposure on Popular Platforms**

****

**Facebook**

Go To Settings: On your mobile app click on the three-line **More** button or the down arrow upper right corner on your browser.

**Privacy Settings and Tools**

Controls who can see the people, pages and lists you are connected with. **Choices** are: Public, Friends, Only Me

Do you want search engines outside of FB to link to your profile – **Set to No**. Prevents your Facebook profile showing up in Google or any other search engine searches.

**Timelines and** **Tagging**

**Facial Recognition** – **Select No One** so FB doesn’t use its facial recognition software to try to identify your face in photos others post. Not only a privacy measure but also prevents you from being mistagged in photos not really of you.

**Review posts before they post on your timeline** – By allowing open posting it may look like you agree with the post subject. **Turn On**.

**Ads**

**Your Information** - FB can target ads to you based on what you listed as your job title, where you work, education, relationship status, or liking a page. **Toggle off** the personal info you don’t want them to use to target ads.

**Ad Settings**

* Ads based on data from partners –Uses data that advertisers and other partners provide FB about your activity off Facebook Company Products.
* Ads based on your activity on Facebook Company Products that you see elsewhere- websites, apps and devices that use FB advertising services, FB uses data about your activity on Facebook Company Products to make them more relevant.
* Ads that include your social actions- your social actions on ads, such as liking the Page that's running the ad. Who can see this info?

Select **Not Allowed**

**Apps and Websites**

You can see lists of every app that you have agreed to use in tandem with Facebook such as Sign In With Facebook. **Uncheck boxes** of apps you no longer wish to share data. The trade off is more inconvenience since to have to set up an account with password for each site. *Work Around* – set up a dummy FB account that only you can see and use that account with no friends or posts for integration.

**General** – Download your FB information to see what they have on you. Takes a little while.

**Settings>Media and Contacts>Browser – on mobile app only** clears the history of websites you’ve visited while browsing Facebook. **Choose Clear Data**

**On you iOS phone - Settings>Privacy>Location>Facebook>Never This way F**acebook can’t track where you are whenever you use the mobile app.

Read more at: https://whatsyourtech.ca/2018/06/21/how-to-increase-and-take-back-your-privacy-on-facebook/

**Twitter**

**Settings menu** – Gear Icon on phone, Profile image on browser

**Security and Privacy**

**Login Verification** - so no one else can hack your account and post as you. Pro – May not prevent hacking but can prevent hacked posting. Con – requires you to give Twitter your phone number

**Limit Photo Tagging** – to only those you follow or no one.

**Protect Your Tweets** – Allows only those you know to see your tweets. Prevents public debacles.

**Tweet with Location** - Don’t check this box if you wish to remain “off the grid.”

**Discoverability** – Let’s others find you by email address or phone #. Requires you to give this personal data to Twitter. Who really wants to be found this way? Don’t check

**Personalization** – Allows Twitter to use information from other browsers and devices you use like search history or location to personalize your experience. If you are concerned about privacy you can’t have personalization. **All boxes should remain unchecked**.

**Browsers – Which One Is Better For Privacy**

*Below is a short answer. For more information go to*

*https://lifehacker.com/which-browser-is-better-for-privacy-1525895782*

*https://www.eff.org/search/site/browser%20safety*

**DuckDuckGo –** Does not track you. It has most of the form and functionality of Google or Bing making it a great option for those who are concerned about their privacy.

**Google Chrome-** Best not to use at all, but if you must, keep in mind the more features you use (voice search, grammar/spell check, bug reporting, user stats etc.) the more Google will know about you.

**Turn Off Google Location Tracking** – Not easy to do, but here is how.

Sign in to your Google account on a browser on iOS or your desktop, or through the Android settings menu. In the browser, access your account settings by finding **Google Account** in the dropdown in the upper right-hand corner, then head to **Personal Info & Privacy**, choose **Go to My Activity**, then in the left-hand nav click **Activity Controls**. Once there you'll see the setting called **Web & App Activity**, which you can toggle off.

On your Android phone, go from **Google settings** to **Google Account**, then tap on **Data & personalization**. You'll find **Web & App Activity** there.

To stop that tracking, toggle the blue **Web & App Activity** slider to off. Google will then give you a popup warning: "Pausing Web & App Activity may limit or disable more personalized experiences across Google services. For example, you may stop seeing more relevant search results or recommendations about places you care about. Even when this setting is paused, Google may temporarily use information from recent searches in order to improve the quality of the active search session." Yes Google, that’s the point.

https://www.wired.com/story/google-location-tracking-turn-off/

**Mozilla Firefox –** They don’t collect as much data as Chrome so their user settings interface is easier to navigate. Like Chrome they are open source so we know what they collect.. They have private browsing which does a little to protect your identity, but some data is still gathered and you lose your browsing history by using this feature. All information sent is on an opt-in basis, not opt out so your level of privacy is mostly up to you.

**Apple Safari** - has a global privacy policy, as well as a commitment to customer privacy that actually gets them in trouble with advertisers. Both Apple and Microsoft have bug bounty programs, and they pay out for reported issues. May be safe, but because it is proprietary we don’t know for sure.

**Microsoft Internet Explorer** – like Safari they are closed source so we don’t know as much about what they collect and how. They also have bug bounties and a Tracking Protection List that EFF praised.

**Opera** – semi-open source. Their malware protection collects your web visit info on their servers, supposedly anonymized. You can turn off malware protection if you are concerned about privacy but you lose the protection. Does offer private browsing.

**A Word About Browser Extensions**

Ad and script blocker extensions give you control over your browsing experience. They can block ads on the sites you visit and kill third-party scripts and widgets that send your data to who knows where. However, if you don’t know how to use them, these tools can render some sites unusable until you figure out what to allow and what to block.

**AdBlock Plus** (Firefox/Chrome/Safari) blocks banner ads, pop-up ads, rollover ads, and more. It stops you from visiting known malware-hosting domains, and also disables third-party tracking cookies and scripts.

**uBlock Origin** – Chrome/Firefox, just as powerful as AdBlock Plus—perhaps moreso, because it gives you more control over what’s blocked and what’s allowed than ABP does also much lighter on system resources, and it doesn’t come with some of the issues ABP has with companies paying the makers of ABP to let their ads through. The only reason uBlock Origin isn’t our top pick here is because it’s a little advanced for novice users, and it blocks a bit more than ABP does, so you’ll need to get your hands dirty to really customize it

**Is Legal Protection Possible?**

Ohms has already said that when it comes to regulation, there will be no way to guarantee maximal usefulness and maximal privacy at the same time. But what is being tried right now? How successful is/will it be?

**GDPR (General Data Protection Regulation)**

This EU law is impacting companies around the globe. GDPR says that companies must obtain affirmative consent to use European residents’ personal information, and when they do, the consent can’t be made a condition of using a service. People who are covered by the law can ask to see all of the information that a company has about them, and they can ask that the information be corrected or deleted.

In addition, people can ask that companies not use automated processes when making big decisions about them, such as financial or legal matters.

Those aren’t the only responsibilities companies face. They must limit their data collection, taking only what’s necessary to do the job at hand, and must delete information about people as soon as it is no longer needed. Businesses also have to give individuals clear and understandable explanations of what they do with their data and why. What’s more, in broader terms, the companies need to do impact assessments to see how their new products or services are going to affect privacy.

It’s still too early to know the unintended consequences of this policy, but American legislators are starting to take a look.

**BlockChain Technology For User Data Control**

A few companies like Ocean Protocol and Revel are working on the idea of using block chain technology, where there is no single company in charge of collecting or holding data (like Google or Facebook do) to provide a platform where people with data can meet. Users can let their phones or computers collect data which they can exchange for digital tokens. The real promise of this technology is that the data can be stored in an encrypted form so that those using the data to run their algorithms cannot collect or even see it. There are still many technical hurdles ahead for this idea, but it offers the first glimpse of a system where the data generator is in charge of his or her data and may even profit from it. (*see New York Times “Breaking Big Tech’s Hold on A.I. 10/19/18)*

1. https://papers.ssrn.com/sol3/papers.cfm?abstract\_id=1450006 [↑](#footnote-ref-1)
2. https://www.aclu.org/blog/national-security/plenty-hide?redirect=blog/technology-and-liberty-national-security/plenty-hide [↑](#footnote-ref-2)