Winter 12-15-2017

Breadcrumbs: Privacy as a Privilege

Prachi Bhardwaj

How does access to this work benefit you? Let us know!
Follow this and additional works at: https://academicworks.cuny.edu/gj_etds

Part of the Databases and Information Systems Commons, Data Storage Systems Commons, Science and Technology Law Commons, Science and Technology Policy Commons, and the Technology and Innovation Commons

Recommended Citation
Bhardwaj, Prachi, "Breadcrumbs: Privacy as a Privilege" (2017). CUNY Academic Works.
https://academicworks.cuny.edu/gj_etds/264

This Dissertation/Thesis is brought to you for free and open access by the Craig Newmark Graduate School of Journalism at CUNY Academic Works. It has been accepted for inclusion in Capstones by an authorized administrator of CUNY Academic Works. For more information, please contact AcademicWorks@cuny.edu.
A Penny for Your Thoughts
By: Prachi Bhardwaj

Last year, data broker Acxiom – a company in the business of collecting consumers’ personal information and selling it to other organizations – made over a quarter billion dollars in annual revenue.

The industry owes its success to the massive demand for consumer data. Finding out what, where, when, and how various demographics make online decisions within different geographical regions helps companies improve artificial intelligence technology, marketing tactics, and user experience. This practice entails gathering information like IP address, browsing history, and private messages, and an insufficient coverage of consumer rights has given companies the opportunity to collect it all with underwhelming restrictions and repercussions.

“Even the most well-informed and well-intentioned consumers will only have a limited degree of control over what will happen to their data,” Alessandro Acquisti, an information technology and public policy professor at Carnegie Mellon University, said in an email.

Unfortunately, that harsh reality has made many people numb to the idea of signing away personal information. While consumers are fearful of information being taken from them without consent, most are all too easily convinced to give up personal data for free services; a fact that companies can take advantage of because no federal legislation currently exists to dictate how the private sector collects consumer data. The Federal Trade Commission Act comes close, but it wasn’t designed with privacy in mind: Section five enforces companies’ privacy policies, and yet there’s no language in the Act that requires companies to put those policies in place.

The U.S. Privacy Act of 1974 controls how government agencies collect PII, and statutes exist for certain sectors like healthcare (HIPAA), education (FERPA) and financial institutions (GLBA). None of these laws hold private sector institutions (companies) liable the way laws in countries across the world do already:
Where national laws fall short, companies like Facebook, Amazon, and Google will look to state laws – led by California – and industry best practices to govern. And companies doing business online assume some consumers in California, meaning the state law that says companies need to have a privacy policy in place, does usually hold water across state lines.

But trusting a consumer with the task of reading that policy – one which will alter the rights of their personal data forever – is a hefty ask, especially when the consequences are unclear and the result is some form of immediate gratification.

“When it comes to privacy, what initially sounded only like a technological problem quickly becomes upon further reflection an economic problem too,” said Acquisiti. “What are the incentives and the resources for individuals to protect their data? Are those sufficient to fend off motivated third-parties (data companies, hackers, etc) who want that data?”

Privacy Policies in Practice

In her study about “the privacy paradox” – a term referring to the disconnect between an individual’s privacy standards and behavior – Susan Athey looks at the two concepts involved in forming privacy-related rules: notice and choice. The former involves telling the consumer what data will be collected and how it will be used, while the latter gives the user the option to accept those terms.

As part of this study, the unwitting subjects – roughly three thousand MIT undergraduate students – filled out surveys expressing digital privacy preferences, and then received incentives (e.g. pizza) for information disclosed (e.g. friends’ email addresses). Almost the entire group of educated young adults took the incentives offered, regardless of the privacy preferences expressed in the survey.

“These mechanisms may not be sufficient,” reads the introduction of the working paper that Athey co-authored.

Taking the pizza is similar to the choice consumers make when asked to tag a friend in a check-in or in an image on Facebook for more Likes. The incentive is relatively trivial, but for many, giving up something abstract and intangible – like data – is much simpler than giving up physical cash, even if the consumer values both highly.

There are degrees of value, of course. A person values someone else’s contact information less than she values her own, and she values her own contact information less than she values her social security number. Opportunity cost can be gauged similarly: If a consumer is told that the information she shares will go to more parties, she’s likely to share less information. And yet the action of accepting the data policy terms for online advertising purposes is nearly identical to accepting the terms for user experience data collection. Just ask the 1.37 billion daily active users on Facebook or Google who also have an iPhone.
Once a user agrees to an iOS update, Apple has complied with both notice and choice, the same way Facebook has complied with both when a user clicks “Create Account.” But the purpose of the data differs greatly.

“For some companies, the product is the product. So, [a] company like Apple sells you an iPhone. For other companies, the product is the person,” said Peter Swire, professor of law at the Georgia Institute of Technology and an expert on privacy and cybersecurity. “People don’t buy things from Google and so Google makes its money by having information about customers.”

For those who have accepted sharing personal data as the norm, this is a small price to pay for a free and useful service. Still, each consumer has a different privacy-driven fear, and a unique line they’re unwilling to cross.

“I'm very willing to provide my name, my email, where I live, which I presume is the type of information a lot of [companies] have about me,” said Andrew Krasovec, a private equity broker in New York City. “Where it does get a little disconcerting is when it’s a financial institution that may have access or information about certain bank accounts or credit cards, or whatever else.”

Unfortunately, terms aren’t tailored to these lines. Consumers assume total accountability for accepting all-encompassing terms, at a time when doing so is so mainstream and simple to do, that it’s an afterthought.

Consider that, in January 2017, nearly 6 million Facebook users were between the ages of 13 and 17, according to data collected by Statista. Then consider the millions of underage
accounts, the millions of users who got their accounts as teenagers, and the large percent of users who don’t read the terms, even after Facebook shortened it by two-thirds. Companies are following the rules, but the rules clearly aren’t enough because a consumer is still in danger of giving away more than he or she intends.

“This might suggest that consumers need to be protected from themselves, above and beyond the protection given by a notice and choice regime, to ensure that small incentives, search costs or misdirection are not able to slant their choices away from their actual normative preferences,” the paper reads.

The choice becomes even more challenging when the incentive involves the product becoming more useful – especially if that product involves costly hardware.

Policy can be adjusted to protect consumers "from themselves" by placing more restrictions on the way that consumers can accept the terms or by making the terms stricter by default. Alternatively, government could push for consumers to be given the option to make adjustments after data has already been collected.

“I’ve supported, for many years, having baseline federal privacy legislation: basic rights to notice about a company’s privacy policies, a choice before the information goes to a third party, and the consumer access to the information the company has about the individual,” said Swire.

These changes would also allow consumers the opportunity to have a degree of control following breaches on company databases that are out of the individual’s control.

Implementing Repercussions

Andrew Krasovec was required to accept PayPal’s privacy policy when he signed up for the online money-transferring service. Recently, he got a letter in the mail saying that one of its subsidiaries – which had access to his information – was hacked.

“Unfortunately, I think it’s more common than one would hope,” he said. “When I’m signing up for a new service or new technology or whatever it may be, I do understand that my providing them information, and linking different accounts to other accounts, the potential – or the compounding of information – is greater,” he said.

It’s the scariest byproduct of collecting consumer data. With minimal punishments in the form of monetary fines or criminal charges in the U.S., the incentive for managing PII responsibly is keeping consumer confidence; a threat that’s becoming more ineffective as consumers become used to personal information being taken, shared, and used. And the rising power of the biggest corporations makes it difficult for consumers to choose a worthy alternative. Facebook, Uber, and Google have proven the invincibility of such brands in the last year alone.
“It’s definitely something that I think about. I also know that there’s not much I personally can do to prevent a hacker from hacking PayPal or hacking Amazon or hacking whatever other major company there is.”

In the U.S., federal law doesn’t require companies to disclose breaches, but 48 states, the District of Columbia, Puerto Rico, and the U.S. Virgin Islands have enacted legislation that require notification to consumers following a security breach that involves PII. Alabama and South Dakota still have no such law.

Of those with disclosure laws, only eight states have laws about how quickly consumers need to be notified, and the timeline varies from 30 to 90 days. A ninth state, California, only sets a timeline for notice on breaches of medical information.

These timelines (or lack thereof) are in place to keep companies quiet in case law enforcement believes doing so will help keep hackers at bay. It also allows companies the opportunity to decide whether the compromised information – data about individuals not involved in the decision-making process – poses a real threat to consumers.

“My stance has always been and will always continue to be like I’ll take minimal steps to protect my privacy, and that’s because I’ve accepted the fact that my data is already lost. It was lost a while ago,” said Steven House, an email security specialist in the Bay Area. “Probably since the first data breach that took place a decade ago.”

He looks forward to a time when the U.S. implements a law similar to the European Union’s General Data Protection Regulation – a law that holds the company liable by fining the breached party large sums of money.

“They attack the individuals, but what they don’t ever hold liable is the companies that maintain that level of data,” said House. “An individual may hack a company, but instead of saying ‘The company should have a better level of security in play to help the end user,’ they say, ‘That individual took that data and he should be held liable, not the company.’”

After accepting a product or service’s terms and turning over all rights to the data that identifies them, consumers are also the party most impacted when that data is handled irresponsibly. By increasing the number of consequences for the party managing the security of the data, government could help incentivize protection.

“I don’t know what they can do to reverse the fact that my information may be compromised,” said Krasovec. “I don’t necessarily know what that means either. I mean, maybe it’s just being a little bit more transparent about what type of information they have compromised.”

Instead, PayPal gave Krasovec a year of fraud protection. His data now lost, that’ll have to do just fine.
The Cost of Being Cautious
By: Prachi Bhardwaj

Following the two largest data breaches in history, Yahoo and Equifax took steps to pacify the chaos, but those measures that a company takes to help consumers in the aftermath of a breach are never enough to protect an individual's information.

“It is a really scary thought and I think until you learn your lesson or have been exposed in that way, you'd rather not think about it,” said Abbey Brogan, a public relations specialist in New York City, who has had the good fortune of steering clear of such unwanted activity. “But maybe once you have, it's like ‘Okay, what lesson can I learn from that and how can I be more secure?’”

There are plenty of personal security tools and services available to individual consumers, but the most effective come at a price and – even as more consumer-friendly products enter the market – require some technical knowledge.

“In the realm of privacy protection and cybersecurity, there are a lot of different product offerings out there,” said David Zuckerman of Zuckerman Capital Management. “Behavioral finance has shown that when there is an overload of information, consumers often do nothing, and I do think that there is a fairly wide swath of the U.S. population that falls into that group.”

The complexity of the topic would put a majority of the 77% of U.S. adults who use a smartphone in a more vulnerable position. For employees at companies with well-resourced IT teams, security precautions like encryption services are generally put in place to ensure employees are being safe, even on personal devices. But individuals without a high school degree, a little over half of who own a smartphone according to the Pew Research Center, are more likely to have to pay for security out of pocket, and less likely to have the education or personal experience to make security-conscious decisions.

“I definitely don’t do any technology-based protection,” said Ari Nordsten, a financial manager in San Francisco. Nordsten uses lengthy and complicated passwords, she doesn’t respond to spam emails, uses caller ID numbers instead of the numbers left in voicemails, doesn’t save passwords on her phone, and uses cash at locations she doesn’t trust. Still, she acknowledges that the more technical decisions are out of her expertise. “[Encryption is] out of work requirement, both on my phone and my computer and my iPad. VPN and extra password [changes] are things that would have never crossed my mind.”

For low-income consumers and blue collar employees, the choice becomes whether to save those dollars or to make security decisions they’re unsure of. For social media platforms, consumers have the affordable option of understanding the associated terms and considering the repercussions of publicly sharing data (although pay-for-play social media cleaning services do exist). Cybersecurity, however, does involve investing in the proper tools and care.
“I mean if I could be 100% safe forever on everything, I'd probably pay, I don’t know, like $10 a month because that's akin to what I pay for renter's insurance,” said Nordsten.

After reading a little bit about each category, select a product to see how you much you would have to pay out of pocket every year* to maintain certain levels of privacy, depicted in the bar below. Keep in mind that no combination of these choices will ever get you to 100% privacy.

**ENCRYPTION IS KEY**

If your data is hacked, the files that you encrypt will be by far the safest. Reversing encrypted code is difficult for even a good hacker to do, so find an encryption service for your most important files.

*For the purpose of this activity, all encryption tools are priced at 100 GB of storage.*

**PROTECT YOUR PASSWORDS**

Your passwords should be long and complex, using every requirement allowed. That's easy if you have one password, but ideally each one will be different, and they won’t auto-fill when you open a website or application. You can write these down or keep them in an encrypted document, but that gets tricky if you’re on the move. Password managers help you generate and store passwords in an encrypted database. There are free options, but make sure you consider your needs. Aside from lacking in some features, free password managers tend to limit the number of stored passcodes or the number of devices you can use it on. LastPass provides more than any other free service.

**KEEP YOUR RECORDS CLOSER WITH A VPN**

A virtual private network (VPN) is an encryption tool for internet traffic, that takes data directly from your device to a server, while avoiding unwanted eyes. When you sign up for a VPN service, the provider owns that server, so you’ll want to pick one that’s well-known (for the right reasons, of course). While some services [have unsuccessfully tried](#) being permanently free via ad-support or limited bandwidth, paid services often provide a free trial. Many are wary of free VPN services, with the assumption that the service is getting its money another way, e.g. selling the data that comes to its servers. There is a free service included in the list below just for comparison’s sake, but experts agree that a free VPN service is probably too good to be true.

**Invest in the hardware**

Handling medical, banking, or social security information should be done in the privacy of your home network. If you don’t have internet at home, you’re in the minority. The number of U.S.
adults with a high-speed broadband service dipped in 2013 according to research from The Pew Research Center, but rose again in 2015 – the year Anthem and the U.S. Office of Personnel Management were hacked, each compromising tens of millions of employees’ data. By November 2016, 73% of U.S. adults were home broadband users.

“Those grab headlines get people’s attention, but I think that the disconnect is how to turn that need for better security and protection into action,” said Zuckerman.

The items in this section aren’t annual like the rest. These prices reflect a one-time payment for hardware. The resulting total is how much you would pay in a year.
Looking Forward
By: Prachi Bhardwaj

"Data protection (and privacy management) has become a much larger problem than something consumers as individuals can address," Acquisti said in an email. "While, as consumers, we can do something, adequately addressing privacy has become a societal problem – one only solvable by a combination of regulatory intervention, broadly-reaching technological solutions, and individuals steps."

To give future generations less to think about, there are lines that need to be drawn.

At the highest level, federal legislation will help patch up holes left by state laws or industry-driven guidelines. At a lower level, companies can start considering the possibility of being hacked when making market-driving decisions, and companies leading the way in security can help by making privacy more affordable.

But on the lowest level, it's up to us as consumers to make decisions that will help keep our information – and the information of our fellow consumers – secure.

"As long as individuals around me are fully aware that like 'Don't click links in messages,' or 'I'm not sending you a message from Bank of America to validate my account,' that type of thing, there are things that I can do in the short term to protect myself and the loved ones around me," said House.

There are free resources to help you along the way: Companies that aren't profiting from selling data to advertisers, and nonprofit organizations whose sole mission is to keep our data, ours. The most important thing to remember is that it won't work if it's a small population's effort. Encourage friends and family to use the applications and tools that safeguard your privacy for maximum impact.

At the bottom, you'll find a list of links to products and organizations to get you started. You can choose to donate money, or just promote the cause.

But first, here are a few free tips on ways you can secure your family's digital footprint:

- A fingerprint is more secure then a passcode, but if you must use a combination to get into your phone, use as many digits as your device allows. A four-digit passcode has 10,000 combination possibilities, but a six-digit passcode has 1,000,000.
- Check your devices’ internet networks frequently to clean out the ones that you don’t use on a daily basis. You never know which one you might have logged into in a moment of haste that's been compromised since, or was already unsecure.
- “Another measure that a lot of consumers should take but may not necessarily be taking yet is 2-step-protection for important log ins,” said Zuckerman. Two factor authentication is required by some services, and optional on others, but given the option, you should use it.
- The “S” in HTTPS stands for secure, so if you’re on a website that isn’t using it, use caution.

Products and organizations to keep an eye on:

**Signal** – A free end-to-end encrypted service

**BitClave** – A search engine that allows consumers to manage personal data and opt in to contracts with advertisers to get paid for it

**Epic Privacy Browser** – A web browser that’s essentially always on incognito, since it deletes all browsing data when you close it out

**Haven** - An app Edward Snowden financially supported to turn your android device into a surveillance remote

**Electronic Frontier Foundation (EFF)** – A nonprofit organization that looks at civil rights for issues like privacy and security and the way those rights should be evolving to accommodate a digital world