Operation Ghost:

Data privacy laws and the distribution of your personal information.

Dan Gormley and Kevin Ghee

Fullstack Academy, New York, NY

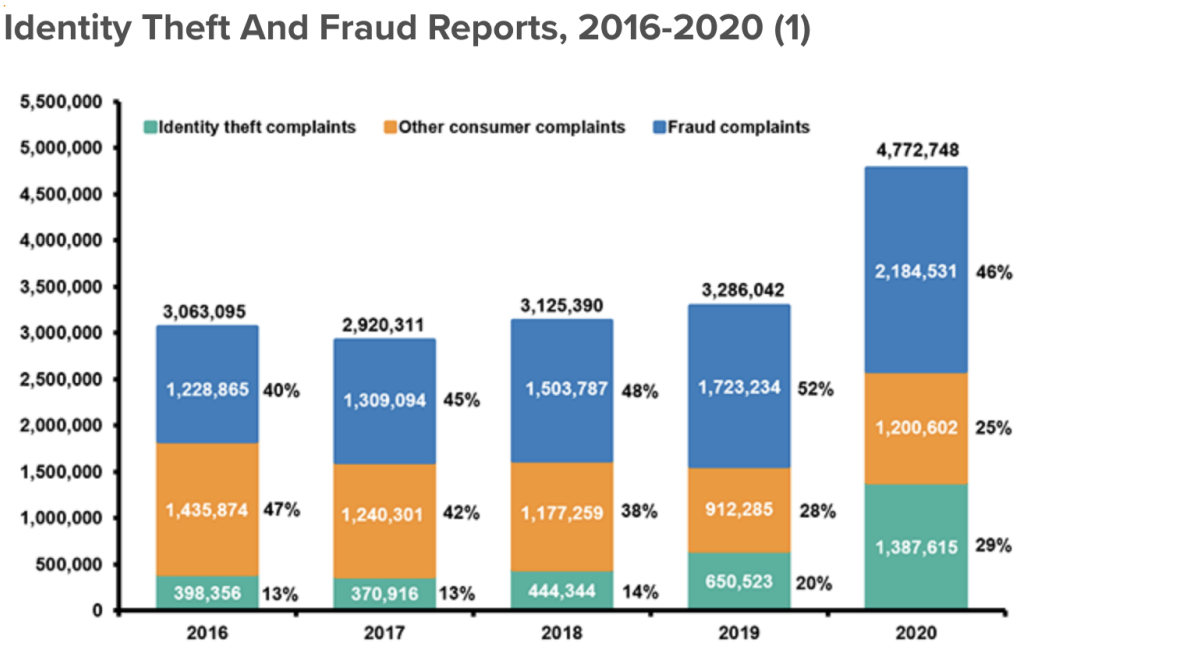
Cyber Bootcamp: Final Project

July 15, 2020

Table Of Contents

CURRENT PROBLEM

Ever since personal data came into existence, there was always a chance that someone's information could fall into the wrong hands and be used maliciously against them. Even before the internet was invented. If someone was able to obtain where you lived via public records, it did potentially cause a threat towards someone's personal safety. The difference between before the internet, and now, is that everyone's personal information is displayed all over the internet for easy access for potential bad actors. With the information shown, just about everyone can be found from a simple name search on these data broker database websites such as Intelius, Spokeo, and countless others, it is no surprise that identity theft and fraud have been on a steady increase over time.



(1) Percentages are based on the total number of Consumer Sentinel Network reports by calendar year. These figures exclude "Do Not Call" registry complaints.

Source: Federal Trade Commission, Consumer Sentinel Network.

It is said that in 2020 alone that 47 percent of Americans experienced financial identity theft and that the losses of these cases in 2019 were $502.5 Billion and rose 42 percent in 2020 to $712.4 Billion. In order to make it harder for a bad actor to obtain information on you, it is imperative to remove your information on these data broker websites that I had mentioned above. It is also long overdue for the United States government to make swift actions and implement law to help prevent this from happening.

PERSONAL EXPERIENCE

As an author of this report I am inclined to share my personal experience when it comes to the release of personal information and being a victim of Identity theft. In 2017 I was working and saving money to lease a motorcycle and then I received a letter in the mail from the telephone provider T-Mobile and it stated that I owed $1600. I was taken away from this information as I have never used their phones or services before. This bill was a negative mark on my credit report which hindered me from getting a loan. My immediate response was to contact the company, dispute the bill, and clear my name. I was told they needed proof and the only information I could provide was my license to verify that my address was not connected to the contract. Yet that was not enough, I was informed that I would need a police report proving that I was a victim of Identity theft. This began the vicious cycle of the police needing proof from T-mobile and T-Mobile needing proof from the police. Thankfully after expressing the frustration and conundrum I was in, the detective was able to produce a blank police report as there was no evidence he could use to investigate further, thus giving the phone company a

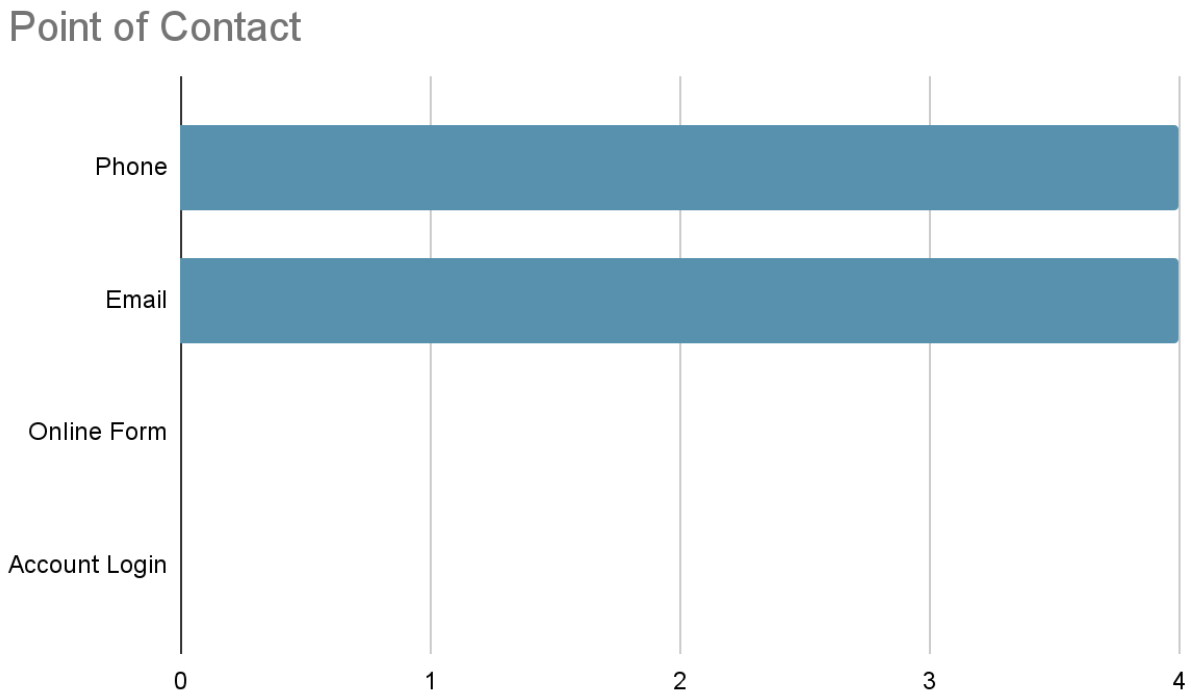
case number that allowed them to verify I was in fact a victim of identity theft. This process lasted 3 months. With relief I was able to get a loan for a motorcycle and ride away free. Little did I know that it wouldn't be the last time it would happen. I received a call from my mother in 2019 that there was an angry repo man with a tow truck in front of her house looking for a black BMW which had an outstanding payment. Once again shocked, I answered that I didn’t own or sign any contract to purchase or lease a car, no matter how nice of a car it was. This began another loop of inquiries and evidence that didn't add up. After reaching out to the dealership I was sent a copy of the contract which didn't even have my correct signature. I also learned that they didn't have a copy of my drivers license. I used my past experience to leverage myself out of the mess I didn't create. Once again free, but wouldn't you know a year later, another identity theft case with another telephone provider. With these experiences I was only notified after the damage was done which gives the perception that I am in fact guilty and only making a false claim to defend myself from a very high unpaid bill. I have frozen my records and identity, removed all unknown addresses and accounts from my records. I can only hope that my bag of tricks will save me from yet another attack.

WE DECIDED TO GO AFTER THEM

In spite of these attacks and fear of our personal information, co-author Dan G. and I decided to take matters in our own hands. We began by searching for companies that display our personal information online in hope to remove ourselves from their sites. The 12 companies we chose to get our information removed from were:

1. BeenVerified
2. Intelius
3. Family Tree
4. PeekYou
5. People Finder
6. People Finder(s)
7. People Smart
8. Private Eye
9. Public records 360
10. Radaris
11. Spokeo
12. USA People Search

We began by searching for opt-out instructions on all the sites. Some sites were straightforward while others needed you to fax a signed form or communicate through an internal messaging system. After opting out as many as we could, we emailed each company and asked them where they obtained our information from? Do you pay for the information or gather it yourself? Have I been removed/will I be repopulated? Who are the affiliate companies/websites? If they understand that information being public is a personal threat, and if they sell our information?. We only received 2 responses and both of them were similar as they stated that all the information on their site has been compiled from public records.



WHY STOP THERE

While engaging with these data broker companies such as Intelius and Spokeo, we discovered some interesting information. While having to dig deeper and escalate most of the phone calls to a supervisor, we were able to get them to admit where they source their data from. For many cases they scrape public records such as Local and State Courthouses, City Documents, Supermarket Reward Cards, Utility Bills, Mortgage Records, License Plates, and Magazine Subscriptions. They also scrape Social Media accounts on Facebook, Instagram, Linkedin, and TikTok. Another interesting fact was that many of these data brokers work together and are affiliated with each other. One of them named Radaris actually has a list of the sources they use on their website.

Here is a list of Radaris' most common public records sources:

- LexisNexis Inc
- ChoicePoint Inc
- Rapleaf
- Datalogix
- Epsilon
- Transunion
- Reed Elsevier
- Spokeo
- Intelius
- Acxiom
- Experian
- Equifax
- USPTO.gov
- Imdb.com
- Amazon.com
- WhitePages.com
- USssearch.com,
- Bing.com
- Classmates.com

Cont'd

- Google.com,
- PeopleSearch.com,
- PeopleFinders
- PeopleWise.com,
- ZabaSearch.com
- Facebook.com,
- LinkedIn.com,
- Wink.com.

As you can see on this list, they use other data brokers as sources for their own data. PeopleFinders, PeopleSearch, USsearch, WhitePages, ZabaSearch, Spokeo, and PeopleWise are all data brokers that provide the same type of service as Radaris. So simply removing your data off of Radaris, and not from one of the others is almost like

running in a circle. They claim that once you remove your data that they will "*try*" to not repopulate a profile of you, but as you can see all they would have to do is scrape the data off of for example Spokeo and your information could be right back on Radaris. An interesting conversation with a Radaris supervisor led us to believe that he didnt see how the service they provide could put someone in harm. Yet when asked if his information was on the site he answered that he had it removed. When following the trail of companies and affiliates, we stumbled across the exclusive purchaser of personal data. The company is Commision Junction, their source of income comes from packaging data for other companies to purchase and use to create and design products to influence consumers to purchase their goods. I believe we found the cycle of personal information and the way it's used to keep individuals spending their money and following anything that is advertised or marketed to them. Therefore any information you put out or found of you is used back against you.

HORROR STORIES

Even though companies claim that their services are intended for good, that doesn't stop the fact that they can be used for malicious intentions. With all the companies sourcing, packaging, and selling your information, you might ask yourself what's the worst that can happen? A quick online search led me to countless victims' stories of having their information stolen. There were multiple cases of family members taking their SSN, licenses, and even credit card numbers to open accounts, purchase cars and even rent an apartment. These stories can be found at…..With all that we now know of these companies let us paint a broader picture of the extent of how an attacker

can use the information found online to harm or endanger you. For example if you happen to cut someone off on the highway while you're driving and the victim wants to settle the score, they could follow you wasting gas and deviating from their original destination, or simply take down your licence plate and enter it into a site and find your place of residence. There is also a service named radar that Radaris offers, where you can put your own name on a list and if there is any mention in a publication, news, references, reports, video or photos then you will be notified. Now let's look at this service from an attacker's perspective. This free service allows an attacker to make a list of people or even a family they want to find and follow. So if you or your family make or are mentioned on a youtube video, take a picture at a baseball game, win a pie eating contest and their name is in the newspaper; the attacker will be notified of when and where the source comes from. Lets hope you or your family members are not on the attackers list.

U.S. AND INTERNATIONAL COMPARISON

As far as the Federal Law goes in the United States, there is nothing in place that provides a central Federal law about privacy like Europe has. Federally we only have verticals of privacy laws. First we have the US Privacy Act of 1974 which was for the rights and restrictions held by government agencies. More specifically, the right of US citizens to access any data held by government agencies. And a right to copy that data. The right of citizens to correct any information errors. Agencies should follow data minimization principles when collecting data – least information “relevant and

necessary” to accomplish its purposes. Access to data is restricted on a need to know basis – for example, employees who need the records for their job role. Sharing of information between other federal (and non-federal) agencies is restricted and only allowed under certain conditions. Next was HIPAA, in 1996 which was the Health Insurance Portability and Accountability Act which contained a data privacy rule stating The Privacy Rule contains a convoluted list of rules on who gets to see protected health informationI. But in short, a healthcare provider or “covered entity” more or less has permission to use patient data if it’s related to “treatment, payment, and health care operations.” However, using the data for marketing purposes or selling the PHI requires explicit authorization. Following HIPAA came the Gramm-Leach-Bliley Act or the GLBA in 1999. Its main purpose is to protect non-public personal information. There are problems with the GLBA for example, many banks will give you an option to opt out of them sharing information with non affiliated third parties, but the catch is there is no way to opt out of them sharing your information with anyone that falls under the “corporate family” which is a major loophole in the law. Lastly we have the Children’s Online Privacy Protection Act or COPPA which is meant to protect the personal information of children under the age of 13 without verifiable parental consent from online companies. These Federal laws are industry specific which should be a concern for the reason that everything else is essentially unregulated, especially if the state you reside in has no state laws as well.

When it comes to state data privacy laws in the United States only a few states have current laws implemented. Those states are California, Virginia, and Nevada. California has the CCPA which was signed into law in 2018. Under the CCPA

consumers have the right to request any personal data that is being held by a covered business. The businesses can't sell your personal information without asking for permission and making a clear attempt to let you the consumer opt out. The CCPA defines personal information as "information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household." Which is a very broad definition that covers a lot of ground. Virginia's law is the CDPA which gives consumers the right to access, delete, correct, and obtain a copy of personal information that covered companies hold on them. Nevada's law allows consumers the right to opt out of the sale of their personal data to third parties, and also made an amendment recently to widen the scope of the law which will be implemented by October of 2021. Many other states do have some type of law but they aren't necessarily as effective as California's CCPA, which should be the model as of now. In fact, many states do have new laws that are currently in the pipeline that will hopefully be a step in the right direction.

THE FUTURE AS WE SEE IT

How does one look to the future when there are so many states and companies not abiding or conforming to the latest privacy rights laws. We believe that in a perfect world that protects the release of personal information and data, it would need to have a list of privacy rights compiled from multiple states and countries. A start to this list would come from Europe's GDPR where it states that no information or data can be stored or collected unless the individual gives consent. One of the other great features of the

GDPR is how they use the data authorities, which requires any company to immediately report any type of data breach that has occurred. It also requires them to report the breach to its consumers as well. This feature is important, as the quicker a breach is recognized, the quicker the data can be recovered and not get into the wrong hands. There are a few states in the U.S. that have adopted certain features of this law, one being New York, but still falling short of the mark of true safety. To add to the list of rights we believe the COPPA should be a part of anyone's laws as it limits the information companies can compile of children under the age of 13. The rest of the laws will read as followed:

- Data brokers should not be able to be used publicly, but only as a resource for legal matters.

- Internet broadband providers should not be able to disclose, sell, use or permit access to any PII. services such as web browsing history, geolocation data, device identifiers and a number of other technical data points that can be used to identify individuals. -Maine Act to Protect the Privacy of Online Consumer Information
- For any company found selling information a fine will be in place for twice the amount of the total sale of personal data.
- Any employee found responsible for the breaking of privacy law will be faced with jail time.
- The right to request any data or information that a company has compiled of them. If those rights are violated, consumers can sue. -CCPA
- Data that is stored by a company should only be stored for a set amount of time before it has to be destroyed.
- Consumers have the right to access, correct, delete, and obtain a copy of the personal information that all public and private businesses hold about them. -CDPA, PIPEDA
- No company public or private can monitor or access an individual's email or computer communication without personal consent.

At the end of it all, it comes down to the choice that an individual has to decide what they consider private or public, and to not have that choice made for them. One of the steps to deal with companies not following the laws, is to have mandatory training of staff and personnel on which laws they must be following in order to not mistakenly release data they shouldn't. All companies, public or private, should be educated on all the privacy laws around the world so that they can prepare for them if the state they operate in adopts them. The effects of these laws being in place will solely impact the way companies conduct their business and ultimately disrupt their bottomline. As technology grows at a rapid pace so should the laws and as of right now that hasn't been the case, which gives companies a fair chance and the legal rights to bend through the cracks to obtain and sell our information. Until all these laws are in place no one will ever have their information completely private and will not ever truly reach Ghost Status.

EMAIL SCRIPT

Request Email for Removal

To Whom it may concern.

As per your privacy policy, please remove my listing from (Company name) and all other affiliated people search sites. Also can you provide me with the name of the company you received my personal information from, so that I can remove myself from future search listings. Please respond within a timely manner,

Thank you for your help with this personal security issue.

Request Email for More Information

To whom it may concern,

Thank you for allowing me to remove my listing, just some follow up questions as I take my personal security very seriously.
Where was the information on your site obtained from? Do you pay for the information or do you gather it yourself. If my records are removed will they be repopulated? As it could have potentially been used against me in identity theft or personal harm, this information should not be publicly available on your website to anybody. I am concerned I will now be having to check your site frequently to make sure I am not on there again. Please respond in a timely manner.

Thank You,
Concerned Customer

BIBLIOGRAPHY

Bekker, Eugene. “Identity theft-odds-identity-theft-statistics.”

https://docs.google.com/document/d/181_IxhvIdhMX6zEv6SNs-3iSdieZabhelfKrWHb-p88/edit,

15 April 2021,

https://docs.google.com/document/d/181_IxhvIdhMX6zEv6SNs-3iSdieZabhelfKrWHb-p88/edit. Accessed 13 July 2021.

“Complete Guide to Privacy Laws in the US.” *Varonis*, https://www.varonis.com/blog/us-privacy-laws/.

“CSO's Ultimate Guide to Security and Privacy Laws, Regulations, and Compliances.” *CSO*, https://www.csoonline.com/article/3604334/csos-ultimate-guide-to-security-and-privacy-laws-regulations-and-compliance.html.

“Facts + Statistics: Identity Theft and Cybercrime.” *Insurance Information Institute*, https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime#:~:text=Additional%20resources-,The%20scope%20of%20identity%20theft,to%20%24712.4%20billion%20in%202020.

“List of Sources.” *Radaris*, https://radaris.com/page/List-of-Sources.

“People Who've Had Their Identity Stolen Are Sharing Their Experiences And It's Mildly Terrifying.” *Buzzfeed*, https://www.buzzfeed.com/meganeliscomb/identity-theft-victims-stories.

Rashid, Fahmida Y. “How to Scrub Your Private Data From 'People Finder' Sites.” *CSO*, https://www.csoonline.com/article/3173231/how-to-scrub-your-private-data-from-people-finder-sites.html.