**Name:** CENSORED

**Date:** 10/1/19

**Class:** COMP-4730

**Assignment:** Case 1

**Case Study Description**

When a computer crime is committed and the perpetrator is caught, they are usually charged with a standard crime alongside one for misusing a computer; in most cases, this is what happens to people who are in possession of stolen data. These rules usually have exceptions, and this is one of those cases – websites like <https://www.haveibeenpwned.com/> and <https://www.weleakinfo.com/> possess databases of information that have been stolen from other websites. These services are hosted under the guise that access to information should be free, so they can possess the data and display it to users. The two websites are different in the way that they display the data, and I will talk about this more in detail in the next two paragraphs.

The first website, haveibeenpwned, is a website that will allow you to search for specific email addresses through a list of breached sites. It will return what breached websites your email was shown in, so that you can hopefully use it to secure yourself. Breached websites are any websites that have had the database(s) holding sensitive information released to the public; these usually contain usernames, email addresses, IP addresses, passwords, and other sensitive information. The catch on this website is that it will merely display what websites your email was found in; it *will not* show you what information was stored in those websites. This is arguably done to prevent attackers from discovering your information, but the problem is that attackers *can* get this information if they need it. By merely masking the data, all it is doing is causing attackers to have to use a different service to discover that information (which is a rather easy task).

The second website, weleakinfo, is a website that will allow you to search for a variety of things: email addresses, usernames, passwords, hashes, IP addresses, names, phone numbers, or even specific website domains! The catch here is that this website *will* return the specific results that are stored within the databases. This means that entries containing sensitive information on you is accessible to strangers for a small amount of money per month! These services exist all over the internet and might seem very scary at first, but ultimately have their own good uses as well. Internet vigilantes use these services all the time to reveal information on criminals and missing/unidentified people, and government employees use these types of services as well. Some people even use these services to strengthen their own security; by seeing the specific information stored in websites, they can figure out which things are visible to the world and need to be changed/secured.

These services are offered on the surface of the Internet, for everybody to use and discover. This means ordinary teenagers can discover social security numbers and credit cards in your name with just a few clicks. While this shocking information is sure to frighten people, the good news is that it helps people everywhere. Seeing the dumped data can help researchers determine which passwords are used the most frequently (and can therefore block them being used on websites in the future) and help people make smarter decisions with their data footprints. This is also used so that websites can understand why it’s important to safeguard their user data. Unfortunately, breaches happen daily, but there is a lot we can do to prevent them. Using password storage software like KeePass can help you use a randomly generated password for each website and manage them all with one single secure password that you know. This stops attackers from being able to use these services to target specific individuals and helps strengthen Internet security at the same time. This combined with good Internet safety practices can help users stay safe from data breaches and attackers.

**Name:** CENSORED

**Date:** 10/1/19

**Class:** COMP-4730

**Assignment:** Case 1

**Case Study Analysis**

There are positive and negative implications that come with the ability to access all this data. While it is okay for websites to host this information for people to search through, it is still highly illegal to use this information for stalking, harassment, or any form of illegal activity. One entirely negative thing is that criminals can hide themselves with sophisticated technology, so they can usually get away with misusing this information for personal gain. Then why is it okay for the websites to host this information? Are we allowing the misuse of this data by making it public, or are we doing this to hopefully eradicate the ability to misuse this data? I will attempt to answer these questions through my next few paragraphs.

There are some positives that come with making this information public; I discussed some of them within my Case Study Description (Internet vigilantes, strengthening your own security with the data, researchers using the data for studies, etc.). The freedom to post this information is an American right, so we must allow for this information to stay public. It would be an entirely worse scenario if we could not tell what information of ours has been shared on the Internet, but attackers could; that would leave us blind to incoming digital attacks, in a sense. People need to see the information publicly (and sometimes need it used against them) to take computer security seriously. We can hopefully, as a society, use the information to help strengthen future systems and make cybercrime nearly impossible.

The negatives that come with all this information public sadly outweigh the positives; while it can be used for good, it is far more likely that people will use it for bad. The average teenager can now sift through your old passwords and other information and hijack your accounts, just by having a subscription to a website for a low amount of money per month. It is incredibly common for hackers to be teenagers instead of adults, due to the amount of unsupervised time they can spend on the Internet. Most teenagers get on their own personal devices whenever they want for however long they want and can therefore start misusing them in their free time for personal gain. Think about it: if you were young and trapped in a bad living situation and the Internet offered these outlets for anonymous income so that you could leave the situation, would you take it? That is the internal struggle that a lot of teenagers are facing; most of them don’t want to be bad people but end up doing bad things to help themselves. With this information being public to them, they can use it for monetary gain through means of extortion or stealing data. This means celebrities, government officials, children – basically anyone is at risk of being the victim of a cybercrime.

No matter what I argued for in this debate, the sharing of this data should be 100% acceptable and it should all remain public. By making this information public, we take the money out of possessing/distributing copies of it; this makes getting a personal financial gain off the data much harder for cybercriminals. We can also help websites better store/secure their data in the future, so that breaches are much less common. Users can be taught how to keep and use secure passwords so that they are not at risk for cybercrimes, and computer safety will overall increase. This has an overall positive impact on the world and will benefit future generations to come, so we should continue making data breaches public. While cybercrime is never guaranteed to die out, we can at least take measures to make it harder to perform so that it becomes less of a worry for ordinary people.