

Security by Infobesity

Security by Infobesity is a theory that people can keep themselves safe, by flooding the world's information systems with all their personal data. Infobesity is the combination of the words, information and obesity, simply meaning information overload. This concept originally was depicted in a book called "Future Shock", written in 1970. This book was so popular; it was reprinted twenty times over a two-year period. The book concentrates on human information overload. Several experiments were done to confuse humans into picking incorrect answers to common questions (Toffler, 343-365"). In the years between that book and the invention of computers, the theory was aimed towards human information processing. A person could conceal his or her actions by supplying overwhelming false information for someone to have to sift through. This method has worked so well, it has been the basis for a lot of embezzlement or fraudulent schemes.

The American public thinks it should protect and hide all of its personal or sensitive data. A proposal for a new personal security tactic needs to be examined. Older ways of keeping safe may no longer be valid. The public needs to put his or her entire life on the web; this will help hide it from anyone who wants access to it. The mass amounts of data collected every year is increasing exponentially. The more online accounts that a person can flood with erroneous information, the safer they will be. When a person does a web search, they should search for ten times more topics than they actually are interested in. When they open an email account, they should open multiple accounts with slightly erroneous information added. This would bloat a person's digital footprint to the point that it appears corrupted, and unreliable. In other words, it would allow the person to hide in plain sight.

The business and political machine tells people to hide their personal information. Companies like LifeLock offer several pay services to keep personal data safe. A person can find themselves paying as much as three hundred dollars a month for these services (Enrollment). It seems to be a conflict of interest for a company to ask for all your personal information, so they can protect it. If you had not given it to them in the first place, they wouldn't need to protect it. Maybe a person should give it to all the companies that want it.

An article in the Washington Post depicts how even famous quotes from people, like Martin Luther King Jr., have been changed in content by something as simple as them being misquoted on Facebook (Bell). Facebook users have been the victims of bogus groups of all types. A large group of scientist was suckered into divulging research information to an unknown data miner, who simply used the name of a top stem cell researcher for his Facebook account (Laursen). A good analogy, made by Mitchell Kapor, the founder of the Lotus Development Corporation, is "Getting information off the Internet is like taking a drink from a fire hydrant (Kapor)." Since these massive amounts of data are suspect in nature, it actually makes finding accurate information even tougher to find than in past years.

Statistics from October 2011 says; 1.4 million total blog posts have been published, over four billion total things are shared on Facebook, and over two hundred million total tweets have been tweeted (Miller). As of October 2012, twitter receives an average of fifty five million tweets a day (Twitter Statistics). That comes out to nineteen billion tweets a year, or almost three tweets for every single person on the planet. With data inputs increasing ninety five times in a single year, the data systems are overflowing with information, most of that data can just be categorized as garbage. But never the less, companies store all this information as a profile on the user for future reference.

A scenario to consider is: if you search for a needle in a haystack, at least you know what the needle is supposed to look like. You can even implore some fancy search equipment to help find it. Now consider searching for a needle in a needle stack. How do you know which needle you are looking for? They all look the same, and are made of the same material. When data is concealed amongst other similar data, it becomes increasingly harder to search through. A man named John Smith would be difficult to find, due to the 25,255 of them listed in the United States white pages (Names). Hence, looking for a John Smith in a pile of John Smiths is almost impossible.

Websites such as www.inteligator.com boast that they can search over one billion records, on fourteen different aspects of people's lives (Intelligator). An average search only takes about thirty seconds to run. Services like these are making a fortune, charging people for what maybe good or erroneous information. The more information that is fed to these databases, the more skewed the results people may find. The FBI, DMV, CIA, and data companies like Lexus Nexus, maintain huge independent databases. These databases are outside the Twitter and Facebook type data companies. This data is actually easier to corrupt than one might think. Misspelling your name on any official document will create new entries in databases such as the one kept by Lexus Nexus. Since the FBI has been rumored to have a file on everyone. Even though they say this is the third most common misconception people have (The Top Ten Myths). Why not add some pages to that file. If a person buys and sells a lot of personal vehicles, their DMV record would already be bloated. As for the CIA, who knows what they are keeping.

Another way people's data is getting propagated to large databases, is through Internet browsers that have direct hooks into certain email systems. A good example of this would be to use Google's web browser called Chrome. Chrome will ask you to sign into your Gmail account

repeatedly during usage. While you are logged in using this service, Google has admitted to recording every single web search or website you visit. They use this information to intelligently market goods and service to users. Google is also the first to admit that they are turning this information over to the FBI at a rate of about two thousand request per year (Godoy).

Looking back at all the information that has been presented in this writing, Security by Infobesity is not as crazy of an idea as one might of thought. Security in the United States is an ever-changing entity. What is a good security method at one time may not be useful at another. We do not use guns or knives to protect our personal interest anymore. We do not use locking filing cabinets, with coded documents in them. The only real ammunition United States citizens have at their disposal is their own personal information. So use this new power liberally and carefully. If information seekers can't figure out who a person is or what they really do, that person will be safer in their daily life.

Works Cited Page

- Bell, Melissa. "Martin Luther King, Jr. misquoted after Osama bin Laden killed", *The Washington Post*. The Washington Post Company. 3 May. 2011. Web. 15 Mar. 2013
- "Enrollment". LifeLock. Web. 15 Mar. 2013
- Godoy, Maria. "Google Records Subpoena Raises Privacy Fears", *NPR*. NPR.ORG, 20 Jan. 2008. Web. 15 Mar. 2013
- "Intelligator, Investigate Anyone: Full Background Check", *Investigate Anyone*. Intelligator. Web. 15 Mar. 2013
- Kapor, Mitchell. "Mitchell Kapor Quotes", Brainy Quote. Web. 15 Mar. 2013
- Laursen, Lucas. "Fake Facebook Pages Spin Web of Deceit." *Nature* 2009. Web. 14 Mar. 2013.
- Miller, Chris "What to Think", *How to Sip from the Information Fire Hydrant*, Cossette. Web. 15 Mar. 2013
- "Names", *John Smith*. White Pages. Web. 15 Mar. 2013
- "The Top Ten Myths in FBI History", *Stories*, Federal Bureau of Investigation. Jul. 2008. Web. 15 Mar. 2013
- Toffler, Alvin. "Future Shock". New York: Random House, 1970. Print.
- "Twitter Statistics", *Twitter*, Statistic Brain. Web. 15 Mar. 2013

Working Bibliography

<http://www.lexisnexis.com.library.icc.edu/hottopics/Inacademic/?verb=sr&csi=279925&sr=HLE>

[AD\(Internet+spreads+erroneous+%27facts%27\)+and+date+is+May+13%2C+2011](#)

<http://www.cossette.com/en/blog/2011/09/13/how-to-sip-from-the-information-fire-hydrant-2/>

<http://www.statisticbrain.com/twitter-statistics/>

<http://names.whitepages.com/John/Smith>

http://www.brainyquote.com/quotes/authors/m/mitchell_kapor.html

<http://www.inteligator.com/home/register.php>

<http://www.npr.org/templates/story/story.php?storyId=5165854>

<http://elitedaily.com/elite/2013/google-admits-fbi-spying-thousands-accounts/>

<http://search.proquest.com.library.icc.edu/docview/204465047>

http://www.fbi.gov/news/stories/2008/july/myths_072408

<https://secure.lifelock.com/enrollment/>