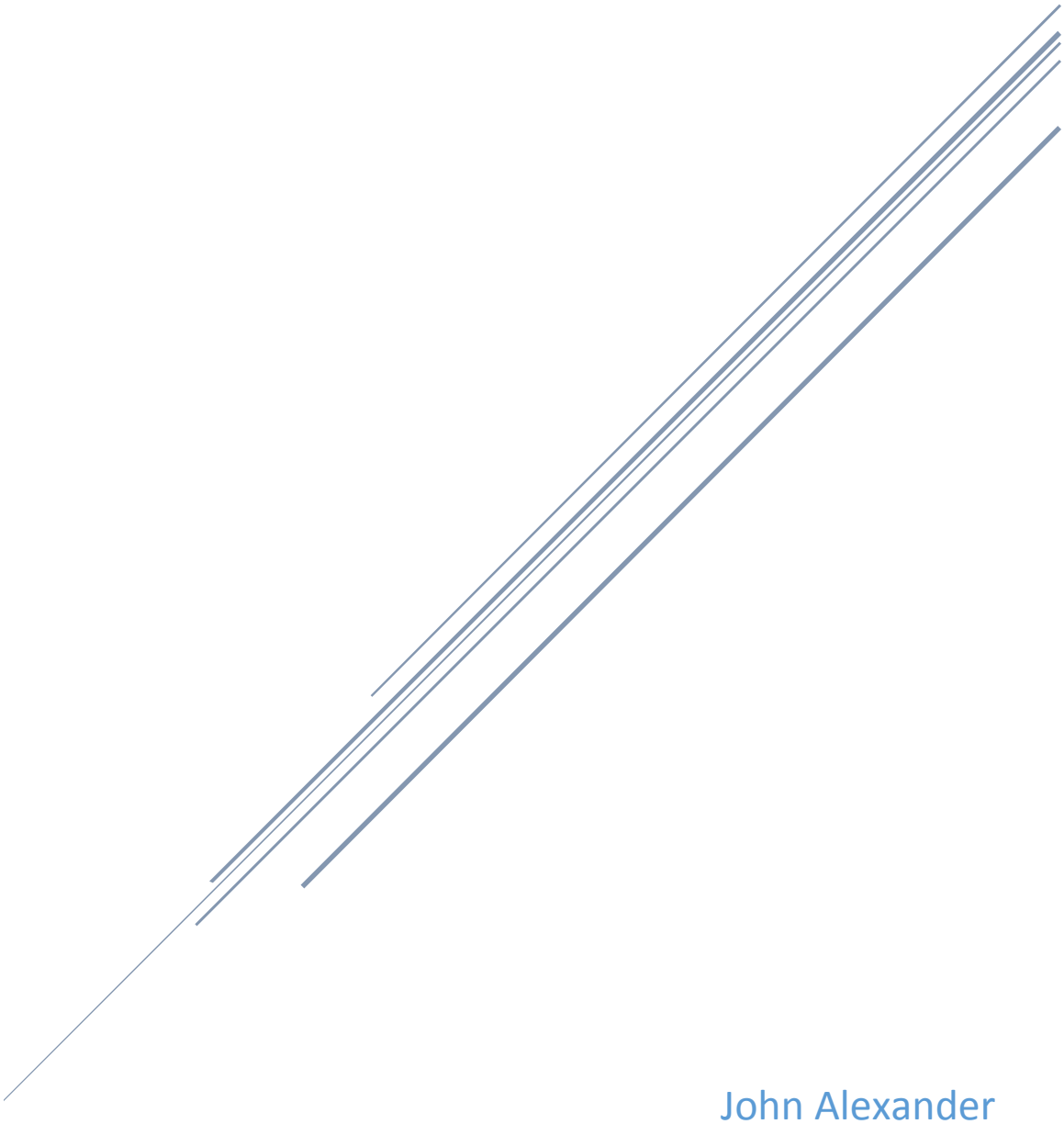
2015

How Technology is Killing Privacy

John Alexander
Grand Valley State University

HOW TECHNOLOGY IS KILLING PRIVACY



John Alexander
April 2015

Privacy concerns seem to come up daily in the news these days, whether it be government spying through the NSA or people willingly giving information about themselves away on social media. It seems as if no one has any privacy anymore. As actor Will Smith said in a recent interview on the show 'Vecherniy Urgant', "I was very dumb when I was 14. See, no Twitter, no Facebook when I was 14. So I was dumb, but I was dumb in private." His view is a common one – that people, especially young people, are being exposed to privacy risks through their use of technology. Willingly given or not the formerly private information of the populace is being stored, tracked, and sold to buyers for both legal and illegal use. Though there are many stories in the news about privacy concerns the general public doesn't seem to be worried, or are perhaps too ill-informed to be worried. Is this problem truly nothing to be concerned about, or is the lack of concern letting this problem spiral out of control?

Defining Privacy

The best place to start is with a definition of privacy in the context of technology. The best way to describe privacy in this context is in terms of "restricted access/limited control" (Tavani and Moor 2001). Restricted access means that there is a form of privacy where some people are allowed access and others are not, so a person can stop others from viewing their information if they so choose. It is reasonable to expect the same amount of privacy in these situations that one would have if not using technology. To ensure control over their personal data, individuals need to have what is called *limited control* over their personal data so that they can ensure restricted access. This can be as simple as being able to toggle privacy settings on a Facebook page. The reason this definition is important is because there has always been a tradeoff between a loss of privacy and a perceived benefit or convenience. If a person doesn't

have ownership of their privacy, they don't have anything to trade within this scenario. However, when using a website, the 'control' a user may feel they have may just be an illusion. Even with all of the privacy settings turned on, there is no guarantee that Facebook isn't going to use your data.

From both the side of the consumer and the companies that want the consumer information, there is a cost-benefit analysis to be done. Every time a person decides to join a new social network, they have decided that they are willing to hand over certain personal information about themselves so they can easily stay connected with their friends and family. They pay the cost of handing over some personal information for what they see as the benefit of being in touch with their friends and family (Ng-Kruelle 2002). A cost benefit like this is totally up to the individual – a person that is very concerned with their personal privacy may not think this tradeoff is worth it and because of this may abstain from creating a Facebook profile.

For a business, the costs and benefits are usually in terms of money, so they are much easier to compare. These services are generally free and make their money from selling user information to advertisers to target ads to people that are more likely to be interested in the advertisement. So the bottom line for the business is seeing if they are making enough money collecting the information of users and selling it to continue to offer the services they provide. If the company can get enough users on its platform, then the tradeoff is usually worth it and those companies stay in business.

As far as a business using services for themselves, they have to deal with many of the same issues that consumers do, except that their data leaks could be worth millions of dollars. Businesses struggle with policies when it comes to cloud services because they need to be ensured that their data is secure. Many software companies are only offering their products in the Software as a Service (SaaS) models, where their applications run on servers that the software company owns. This kind of model means that the company using the software runs the application through the cloud, entrusting the software company to protect their data. Depending on the kind of software, this data could be anything, from customer data to secret information about upcoming products. In situations like these, the benefit is getting to use the software while the cost is the risk of storing their data externally with another company. To mitigate this risk, most companies have strict policies as to what data can be stored externally and what data is only allowed to be stored internally, as well as what cloud services users within the company are allowed to use.

The restricted access/limited control view of privacy can become problematic when it comes to government surveillance, because it isn't always possible to avoid having their privacy invaded. The Patriot Act was a reactionary bill passed after the 9/11 terrorist attacks. It has widely been understood as "a 'sweeping' antiterrorism law that gave the government 'vast new powers' to conduct electronic surveillance over the Internet" (Kerr 2003). Basically the government had the power to search through everything on the Internet under the premise of this act. The only way to avoid government surveillance is to not use electronic communication at all. This situation is a different set of costs and benefits to the average person. You can either maintain your privacy by not using electronic communication; or, you can just accept the fact

that the things you're doing on the Internet/the conversations you're having on the phone could be getting tracked by the government and use these technologies anyway. The vast majority of the population will choose the latter – much to the benefit of the U.S. government. Not using the Internet is out of the question for most people, especially young people. They just accept that they could be being watched, claiming that they "have nothing to hide". They don't realize the value of their personal information, and the benefit of modern technology is so great that the cost of privacy loss would have to be astronomical for them to stop using it.

Who is Taking Our Information?

There are a number of different groups looking to gather information on people, because information can lead to knowledge and knowledge is power. Luckily for the people looking for information, the Internet makes it easy to gather a large amount of information quickly. WikiLeaks founder Julian Assange described the Internet as the "greatest spying machine the world has ever seen" (Kingsley 2011). It is easy to see why he thinks that this is the case. Some of the organizations looking to collect user data are Facebook, Google, and the National Security Administration of the United States.

The National Security Administration (NSA) is an organization that has roots in code breaking in World War I and World War II, but has grown into one of the largest government organizations in terms of staff and funding. There are estimates that say that the NSA has nearly 40,000 employees and an estimated budget of $11 billion, though it is probably more than that (Verble 2014). Following the 9/11 terrorist attacks, the NSA was discreetly authorized to spy on American citizens without a warrant to do so, which has stirred up quite a bit of

controversy. Though the NSA seems to continuously get surveillance powers stripped and then later secretly given back, it seems that the NSA continues to spy on people both domestically and abroad without any public uproar. However, the NSA has been caught spying on foreign leaders – including those that are supposed to be our allies.

Two other major players – Google and Facebook – have similar tactics and similar goals. Both companies provide a number of services to users free of charge, because their primary source of revenue is selling user information to advertisers. These companies have the capability to track user traffic and are essentially giant databases filled with user information that can be mined and sold for a profit. While Google and Facebook aren't the only websites that do this, they are two of the major players that come up when user privacy is discussed. Just to check how much Google knows about you, you can check your 'Google Ads' settings where they use the data they have collected on you to guess your age, gender, and interests. This is the information that Google uses to tailor ads to everyone that uses their services.

What is the Information Used For?

If a service is being offered to you for "free", chances are that you are the "product". Your time and eyes are what are making companies like Facebook and Google money. In the case of Facebook, advertisers pay them for two different types of ads. Some ads are blanket ads that have an equal chance of being seen by everyone. However, most of the advertising money that Facebook is from targeted ads. Facebook searches through the likes and statuses of users to target ads at the people that would be most likely to buy the advertised products. Basically,

the information that Facebook collects on its users is “sold” to companies that want to advertise on their platform.

Google does the same thing with information it has gathered on users, but most of Google’s revenue still comes from sponsored search results. According to ‘Location-Based Sponsored Search Advertising’, sponsored search consists of three parties: “(i) users pose keyword queries with the goal of receiving relevant material; (ii) advertisers aim at promoting their product their product or service through a properly designed ad, and target relevant users by declaring to the search engine a set of keywords that capture their interest; (iii) the search engine mediates between users and advertisers, and facilitates that interaction”(Trimponias 2013). So every time a word is searched in Google, all the sponsors who have paid for a bid every time that word shows up has a chance of appearing as one of the first three searches on the page. If you are logged into Google, your searches are also tracked so that ads that they deem relevant to you can be shown at any time.

Many businesses use data mined from users to look at consumer trends. Programs like Meijer’s “M-Perks” have customers register for a rewards cards that often give them a small percentage off of their purchases. Companies are willing to do this because the information gained from these programs is much more valuable than the amount the customers end up saving. When customers register for these programs, they have to fill out their age, gender, and other demographic information before they receive their cards. The company then links this demographic information to customer purchases that they use to gain valuable insight about what kind of customers are buying what, as well as what items are bought together. Customers

can benefit from this information, as coupons are targeted to them based on their purchases to encourage them to come back to that store.

As it is a part of the United States government, the NSA isn't looking to make money off of the information of the people. The primary focus of the NSA is to protect America from outside threats, which what they do with the information they gather. While many people think the NSA overreach with their methods, supporters say the NSA is "serving as a key bulwark against foreign terrorists and that it would be reckless to constrain the agency's mission" (Gorman 2008). While people like the fact that potential terrorist attacks are being stopped, many are still upset that the NSA is collecting and storing nearly every form of communication imaginable, including phone calls and emails. When it was revealed that the NSA were recording and storing all phone calls, one study found that 59% of Americans disapproved of the US Government secretly collecting phone records (Verble 2014). While some people just like to maintain their privacy, others still are concerned about the data that the NSA has collected getting into the wrong hands and being exploited in some way or released by a hacker, or an insider like Edward Snowden.

Hackers are another class of people that are looking to use the personal information of others. These hackers generally have a more malicious intent than legitimate organizations like Google or Facebook, such as identity theft or credit card theft. The key difference is that while other organizations make money off user data by selling the data to advertisers, hackers are generally trying to steal the money directly from the users. Many people's objections to data collection by anyone is due to these hackers, and therefore much of the security that is implemented is to prevent these sort of attacks from working. When people are up in arms

about the NSA's spying, they are upset because of the invasion of privacy and because of the risk of the NSA databases being hacked, and their information being used for nefarious purposes.

Should we be Worried?

The increase in information gathering, with or without the knowledge and consent of the people whose information is being gathered, is definitely cause for alarm. However, different demographics of people have varying levels of concern when it comes to information privacy. Younger people, for example, are less likely to be concerned about Internet privacy than their older counterparts, even though they are more likely to know that their information is being collected and tracked. Females are more likely to be concerned with Internet privacy than males, and people with more education are less likely to be concerned (Zukowski 2007). Interestingly, the more familiar with the Internet the person seems to be, the more comfortable they seem to be with their personal data being collected.

The issue with user data collection is the risk of misuse, and what different people/companies view as proper use of personal information. For example, insurance companies have been mining for client data to look for possible health risks, and have been accused of changing client rates based on the data they have mined. This is different than a client disclosing their own health risks as the information gathered by the insurance company may be inaccurate, and may lead to clients being overcharged for their insurance. Another situation of a company overreaching is when Target revealed a pregnancy of a teenaged girl to her father when they sent a "congratulations" to her home after noticing that she recently bought larger handbags, tissues, and headache pills. While marketers clearly thought that it was

an acceptable marketing ploy, many people saw it as a clear invasion of privacy and an abuse of data mining (Virani 2015).

Something to consider when you think of your privacy when using the Internet is how these companies like Facebook make money – essentially by selling "you". In fact, Facebook has been caught showing false endorsements from a user's friends for products they have been paid to advertise, and don't tell you when they do so (Virani 2015). What happens in these situations is that an ad will appear on user A's Facebook, claiming that user B recommends a product to them, when in reality user B has probably never used the product being endorsed by "them" and has no idea that their name is being used to advertise a product.

Facebook builds an unnervingly accurate model of who you are as a person by reading your statuses, private messages, and likes. Facebook can also track you on any page that has a plug-in 'like this on Facebook' button, following you around the web outside of Facebook to gather more data on you. All of this data is being collected on users, and Facebook is just one of the many companies collecting data. This is scary, because these companies make money by selling user data, and the laws can't keep up with the technology when it comes to the Internet. Users have no idea what the companies collecting data are going to do with it. It is hard to stop them from doing anything because there are few laws, if any, to prevent the collection and sale of user data.

The fact that companies are making money from your personal information, and that there are very few limitations to what they can do with that information, should be very concerning. In many cases the only thing holding these companies back is the bad PR they

would get if they got found doing something that many would consider to be unethical. Many companies are already doing unethical things (or have the potential to do unethical things) hidden away in long terms of use agreements that no regular user reads. Unless something changes or something is done to stop it, the whole situation could easily spiral out of control and become a much bigger issue than it already is. However, there would have to be a massive push for the protection of privacy from average citizens for any changes to occur. The companies won't back off unless people protest, and the government won't make any laws regarding privacy unless the citizens demand it.

How People and Organizations View Privacy Differently

Where problems usually arise is when the organizations and the users of the organizations services don't see eye to eye on privacy issues. Users are likely to assume that their 'private' information isn't being looked at and used by companies for their own uses, failing to realize that social media profiles are just giant databases waiting to be mined. They believe that because other users can't see their information, no one can. Companies, on the other hand, realize the value of the wealth of information being willingly put places where they can pay to access it. Facebook's privacy policy even says "You give us permission to use your name, profile picture, content and information in connection with commercial, sponsored or related content (such as a brand you like), served or enhanced by us" (Virani 2015). They tell you in their policy that they can share your information with businesses, however many users do not realize that their personal information isn't just for them and their friends when they post in online.

The public's view on the privacy is usually that they would be opposed to companies collecting and using their information – if they knew what was going on. Companies take advantage of the ignorance of the populace to get away with more than they should. For nearly every convenience provided by a free service, there is a price to be paid. Many people choose the "log in with Facebook" option on apps and websites because it's convenient and they don't feel like creating a completely new profile. When users do this, they are giving Facebook more information about themselves. Users need to become better educated on what information is being taken by the services they use so they can better evaluate the tradeoff of the information they give up about themselves and the service provided by these services.

What's the benefit?

While some people have no idea how much of their data is being tracked, others are well aware of what is happening and choose to be apathetic about their information being collected. For these apathetic people, the tradeoff between the loss of privacy and the use of the technology is worth it. If avoiding having your information tracked means that you can't use the latest cool smartphone application, many people will bite that bullet and use the app anyway. To them using the newest and coolest technology is more important than being private. There is a conscious tradeoff between privacy and services provided that many people make on a daily basis.

Beyond the simple fact of using the available services, there are ways that users can benefit from their information being tracked. An example is when there are advertisements targeted at individuals based on the profile that has been built on them – what if they actually

want the product that was advertised to them? People could find products that they are interested in through this type of advertising which is the whole point of the advertisements in the first place. Targeted advertisements are meant to show people products that they would want to buy; and when it works, everyone comes out of the situation happy. A similar benefit are coupons targeted at people based on their interests or past purchases, as consumers can really benefit from the savings available from these sorts of deals. These kinds of coupons are especially prevalent when stores use rewards programs, as rewards accounts are just an easier way to track someone and their purchasing history.

There are other ways seemingly invasive technologies can end up helping users with their daily lives. With tracking technology in phones and cars, there are applications popping up designed to help you avoid traffic and to give you alternate routes around the traffic, such as the popular “Waze” smartphone application (Jeske 2013). As more technology peripherals are developed, more health applications are being developed to track your heart rate, blood pressure, and basically any of the basic bodily functions that you would want to track. This technology could help detect the warning signs of more serious problems and advise you to seek medical attention when needed. However, a downside to this type of information is that it could also be tracked by insurance companies who will raise your rates at the slightest sign of health trouble.

Some other assistive technologies that we willing hand our data over to are financial services like Mint and Financial Advisor. These websites help you manage your money and investments. To use them, users provide access to their financial records, which is some of the most private information that a person has. However, many people have entrusted their

information to these services because the value of the guidance offered is worth the risk of something bad potentially happening to their data. However, there is always a danger of these services being hacked into, or if an employee for one of these companies decides to take user information and sell it to the highest bidder. With nearly every benefit offered by any online service, there are always dangers and tradeoffs that need to be considered – and many people do not.

How to Protect Yourself

The first step in protecting yourself from the dangers of getting your data tracked is making sure you are informed and know what the services you are using are doing with the data you are giving them. You cannot make an informed decision on the tradeoff between privacy and use of a service if you do not know how much of your privacy is being invaded. While it is the responsibility of the companies or individuals to use people's data responsibly, it is also the responsibility of the users to make sure that they are not being taken advantage of. If users do not do their research, they can hardly complain when something they don't approve of is happening with their data.

The problem with the "do your research" method of protection is that many companies make their End-User License Agreements (EULAs) intentionally confusing and full of legal jargon, which often make them hard to read to anyone without a degree in law. Companies do this so that the few people who do read the EULA will likely not understand what it is saying, all while covering themselves in case of a lawsuit. That way, if someone catches the company doing something that seems wrong, the company can often point to a specific part of the EULA and claim that the user agreed to it when they accept the EULA. However, there are often posts

online that break down the more 'interesting' parts of a popular company's EULA into more understandable terms. These are the types of websites the average person should be looking for while they do their research.

There are much more active things that users can do to protect their privacy that aren't simply researching. One of these things is to download browser extensions that can help to stop people from gathering information about you while you can use the Internet. Adblock Plus (available at https://adblockplus.org/) is a browser extension that not only blocks ads from your browsing experience, but also disables third-party tracking cookies and scripts. Websites can host these kinds of scripts and not tell you where they are sending the data they have collected, so blocking them can go a long way in the quest to stay private.

Adblock Plus works pretty well blocking basic tracking, but an extension called Disconnect (available at https://disconnect.me/) blocks third party tracking cookies and gives you control over all elements and scripts on a webpage. Disconnect also stops websites like Twitter, Google, and Facebook from tracking your web presence, both when you are using their services and when you are not. This extension also prevents you from an attack called "sidejacking" where an attacker can use stolen cookies to access your personal data.

There are some other extensions and programs that are worth looking into as well. Web of Trust (https://www.mywot.com/en/download) is an extension that ranks websites by reputation, and will tell you if a site has been reported to have malware. Malwarebytes Anti-Malware (https://www.malwarebytes.org/mwb-download/) is a free program that is very well known for being great at detecting unwanted malware and adware on your system. Looking

into email encryption is worthwhile as well, to protect your emails from prying eyes. A good Chrome extension for this is called Virtru Email Encryption (available in the chrome web store). You can simply hit the 'encrypt' button before sending an email and the email encrypts for you, assuring it safely reaches the proper destination.

The problem with browser extensions, even the well trusted ones that I have listed, is that they often need to collect data on you as well just to function. Many of them (like Adblock) are run off of user donations, but it can view and track all of the sites that anyone that uses it has visited, even if cookies were turned off in the browser. If someone found an exploit or security hole in the extension, then data about you is once again in the hands of someone you don't want it to be in the hands of. Because of this, the best protection is still to be careful and to be informed. There are no amount of extensions or programs that can protect someone if they are being reckless on the Internet. A good rule to live by for watching what you post is to assume that everything that you say on the Internet can be traced back to you somehow. Living by this rule, you can be assured that nothing private about you will be in anyone's hands but your own.

Resolving the Privacy Issue

The issue with the entire privacy problem is how quickly the technology moves compared to anyone's reaction to it. Laws can't keep up because they can take years to get passed and they are no longer relevant if they ever do. Users rarely stay up to date on the newest technologies and often don't realize how much of their information is being tracked.

For anything to change in a meaningful way there will need to be a major change in the mindset for everyone – users, lawmakers, and companies.

The mindset that everyone would need to have to make a difference is that of privacy first, information second. There are too many downsides to this sort of mindset for it to be viable, because the information is valuable to too many parties. For companies, the information is worth money. For some companies, like Facebook, the information of others is their main source of income. For others, the information provides valuable insight into the minds of customers that greatly improves profits. For the government, the information gathered is invaluable to organizations like the NSA and others to fulfill their various objectives. The NSA's entire purpose is entrenched in the information of others, so it is extremely unlikely (and counterproductive to their mission) that the government would do anything drastic when it came to information collection policies.

The only people that could possibly instigate any changes are those who the information isn't worth money to – the users. However, there would have to be some loud voices and some even bigger sacrifices for any changes to be made. No matter how loud everyone shouts, changes will not be made until you hit the companies where it hurts – their wallets. Companies don't care if you disapprove of their methods if you continue to use their products. However, if there are large scale boycotts, that will get the attention of the companies and force them to make changes. Most users would be unwilling to boycott anything, because the services are too valuable to give up for a significant period of time. However, if there really is going to be a change the companies need to be losing money, and need to know that they are losing money because people disapprove of their collection policies. Until that happens, the only way that the

individuals who are concerned about privacy can be safe is to minimize their use of technologies that can be traced and collected.

Unfortunately for those who are concerned about privacy, more companies are now using cloud-based models instead of allowing users to install software locally. This is a move even farther away from privacy, because now these software companies are storing all of the data that is passing through their system. For example, Microsoft is moving away from their traditional model with their Office products with the release of 'Office 365', where all of the software is based in Microsoft's cloud. Many individuals, educational institutions, and businesses use Microsoft Office data, and now Microsoft can see all of it with the default settings. For the near future, it looks as if things are going to get worse before they get better.

Conclusion

A person's privacy is just as valuable as ever, the only thing that has changed as technology as changed in recent years is who holds the value. While each individual used to hold the value of their own privacy, companies now sell private information of others to make money. These companies continue because of user ignorance and user apathy – people either don't know or don't care enough to try to change how the system works. While it may seem harmless to most of the public now; as technology improves, it will only get more and more invasive. The benefits of the technology will improve as well. At some point, the public needs to draw a line in the sand and say that enough is enough.

Until the point where the public makes a stand is reached, the best way to stay protected is to make sure you are well informed about the technologies that you are using.

While companies may try to hide how much of your information they are taking, constant vigilance can help you protect your personal information from those who seek to profit off of it. In some cases this may mean that, to be safe, you may not be able to use the coolest new technology. You need to as an individual take ownership of your personal information and make a conscious decision on what you are going to share and with whom you are going to share it. If you do this, you are trading your information instead of just handing it over. If you choose not to make that trade, then you are telling that company what you think in the most effective way – with your wallet.

When it comes to government spying, it the responsibility of citizens to make it clear that the type of spying that the NSA is doing isn't acceptable. Until pressure is put on lawmakers to repeal the excessive parts of the Patriot Act and to put new regulations in place to describe how much information that government agencies can collect about people, nothing will change. Pressure can be applied in various ways – calling or writing to your local representatives, signing petitions and encouraging others to do the same, and most importantly by voting for those who have the same viewpoint that you do on this issue.

Technology, especially in the past 20 years, has resulted in many conveniences that we enjoy every day. Facebook, Google, and even email are technologies that didn't exist until quite recently, and while the value of these things is great, your value to them is even greater. No matter how many privacy controls you put in place, if you use these services your data can be viewed by the company that runs the service. Oftentimes, they can do whatever they want with that data because of what users agree to in the Terms of Service for their product. No one would go so far as to suggest that we should get rid of these services, but a very critical analysis

needs to be cast their way to see what data is actually being collected. No one truly knows what is happening to the data once it is the hands of these companies. Personal information has value, and should not be given away for free.

Citations

Carani, Salim. "Get Your Loved Ones off Facebook." *Get Your Loved Ones off Facebook.* 29 Jan. 2015. Web. 1 Jan. (2015). <http://saintsal.com/facebook/>.

Gorman, Siobhan. "NSA's Domestic Spying Grows As Agency Sweeps Up Data." *The Wall Street Journal* 10 Mar. 2008. Web.

Jeske, Tobias. "Floating Car Data from Smartphones: What Google And Waze Know About You and How Hackers Can Control Traffic." *Black Hat Europe* (2013). Print.

Kerr, Orin S. “Internet Surveillance Law after the USA Patriot Act: The Big Brother that Isn't.” *Northwestern University Law Review* (2003).

Kingsley, Patrick. "Julian Assange Tells Students That the Web Is the Greatest Spying Machine Ever." *The Guardian* 15 Mar. (2011). Web.

Ng-Kruelle, Grace, Paul A. Swatman, and Douglas S. Rebne. "The Price of Convenience: Privacy and Mobile Commerce." *Quarterly Journal of Electronic Commerce* 3.3 (2002): 273-85. Print.

Tavani, Herman T., and James H. Moor. "Privacy Protection, Control of Information, and Privacy-enhancing Technologies." *ACM SIGCAS Computers and Society* (2001): 6-11. Print.

Trimponias, George, Ilaria Bartolini, and Dimitris Papadias. "Location-Based Sponsored Search Advertising." *Advances in Spatial and Temporal Databases* (2013). Print.

Smith, Will. "Vecherniy Urgant." Interview by Ivan Urgant. *Vecherniy Urgant*. Channel One. Ostankino, Moscow, Russia, 31 May 2013. Television.

Verble, Joseph. "The NSA and Edward Snowden: Surveillance in the 21st Century." *IGCAS Computers & Society* 44.3 (2014): 14-20. Print.

Virani, Salim. "Get Your Loved Ones off Facebook." *Get Your Loved Ones off Facebook.* 29 Jan. 2015. Web. <http://saintsal.com/facebook/>.

Zukowski, Tomasz, and Irwin Brown. "Examining the Influence of Demographic Factors on Internet Users' Information Privacy Concerns." *South African Institute of Computer Scientists and Information Technologists* (2007). Print.