The Battle for Privacy

By

Ricardo Estrada
Many of us never would have known that there is a current legal mess with our privacy and one would not stop to wonder that our privacy is really not our privacy at all. In fact our privacy is constantly being invaded by insurance companies, marketers, employers, data corporations and quite possibly our very own government (law enforcement). Privacy is treated in our society (more than any other) as a highly privileged value. However, there are many issues that are currently a hot topic with the invasion of our Privacy and this paper will focus on several of those topics. I will compare the good and the bad that goes with the use of encryption, the invasion of our privacy when it comes to our medical records and take a look at the use of biometrics cards, are they beneficial? An argument that comes up and seems to justify the invasion of our privacy, according to those who are for our breach of privacy, is using this breach of trust for the investment in the common good, and most specifically about our concern for public safety and public health. It is these same issues that we must take a deeper look into in order to address the moral, legal and social issues that arise when serving the common good entails violating our privacy. It is a question that we must all look into and decide if our right to privacy should be curbed? We will discover that the limits of privacy vary depending on the issue being addressed.

Encryption is the process of transforming information using an algorithm to make it unreadable to anyone except those possessing a key to decrypt that information; it is the most effective way to achieve data security. There are two ways that we can use encryption, the first one can be used for a good purpose, such as securing our information and the second option is the usage of encryption for malicious purposes, such as crimes. It is the second usage of encryption that is putting a good technology under the scrutiny of the government and could possibly lead to an invasion of privacy.
Because of the usefulness of encryption this great tool can bring us peace of mind when it comes to securing our data. It brings up a sense of privacy knowing that our data is safe and that the only way for anyone to access (decrypt) our information is if they have a key that we possess. This possession of a decryption key ensures that our personal information (data) will be safe and inaccessible if it were to ever fall in the wrong hands. “Businesses use encryption to protect themselves against espionage by competitors and foreign governments, and to establish secure links with their partners, suppliers and customers.” (Etzioni) By using encryption, companies can bring a sense of trust with whomever they are doing business with, because they are guaranteeing that the data they posses is secure and will not be breached. I’ve used encryption to pass personal identifiable information (such as social security number) to my employer when I was hired on to work as a contractor. Because of how sophisticated and impossible it is to break the decryption, I trust that my information will not be seeing by anyone else, other than the person that it was intended for. In essence, the true reason for encryption is to keep our data out of the view of unwanted prying eyes.

Encryption greatly enhances privacy in the cyber world, but it poses new barriers to authorities as terrorists, drug lords, pedophiles and other criminals increasingly draw on the new forms of encryption. In other words, technology has a “dark side” and it can also be used by malicious people to commit crimes. Encryption is used by various crime organizations to hide any type of evidence that may be used against them in court. A pedophile may encrypt incriminating images of children that he has in his hard drive, terrorists may encrypt their plans to perform another attack on American soil and pass through email. The lists of hypothetical situations that are brought up with encryption go on and on. It is the severe hypothetical situations that have authorities concerned about encryption. The use of encryption by criminals
can make it impossible to obtain necessary evidence to convict the pedophile, the drug dealer, the terrorist and the other types of criminals. The use of encryption can frustrate anti terrorism efforts since most of the data that can be intercepted, is not readable because of the sophistication of the encryption. These communication intercepts can reveal valuable information about the intentions, plans & membership of criminal organizations and generate leads for criminal investigations. For authorities encryption can hinder the gathering of intelligence and this problem is what may lead to greater violations of privacy from the government. Because encryption may take a lifetime to break, authorities may have to resort to monitoring by surveillance, wiretap, cameras, microphones and thus adding to the invasiveness of someone’s privacy. The Patriot Act can be thanked for removing some of the frustrations involved with encryption. If a person is deemed as a terrorist (threat) to America, even if they have encryption, the government would be allowed to conduct monitoring and surveillance. All of their actions would be justified on the basis of the Patriot Act. Just because a big hypothetical situation (i.e. attack on a building) is possible, should the government diminish privacy to further the common good? I do not have any concerns about my privacy, since I do not have any bad intentions with the encryption software I use. The only reason I use encryption, is to prevent my data from being stolen by hackers or identity thief’s. Should we take such huge steps in diminishing our privacy in order to prevent something that probably won’t happen? The possibility of a catastrophic event is unlikely, but still possible with threats from terrorists. Should our right to privacy be curbed because of the actions of a few people?

Those hypothetical events that arise from encryption are what drive authorities into attempting to invade our privacy with encryption. They have been successful in intercepting and decrypting (because the encryption was not strong) information and successfully foiled some
attacks. However, with the advancements in algorithms for encryption, Authorities have been having problems decrypting information. Public authorities have found that they cannot break the codes on their own. NSA has spent 5 billion dollars trying to break the strongest codes and failed to do so. So with those failures, the government turns to a much cheaper option and states that public safety requires that it be granted, by parties involved, the “keys” needed to decipher their encrypted messages. “A variety of `key recovery,” `key escrow,” and `trusted third-party” encryption requirements have been suggested in recent years by government agencies seeking to conduct covert surveillance within the changing environments brought about by new technologies” (Abelson). This is where the invasion of our privacy is now up for granted.

Authorities are trying to figure out a way to still give users the privacy of using encryption keys while still having a copy of the “keys” through a third party. This possession of someone’s decryption key would give authorities access to someone’s personal data when they are conducting some type of investigation on them. This is called “public key recovery” and the data that they would be accessing is email and stored files. However, this is not an immediate invasion of privacy. The authorities would have to get a warrant from a judge in order to proceed to use the “key” we supplied them for the purpose of monitoring us. Once they have a warrant, we would be considered according to authorities, as suspects. But opponents of this argue that they can get, just as reliable encryption from foreign countries with no “public key recovery” installed. The problem here is that the government would then have to resort to banning the use of not approved encryption software in order to keep the public within the constraints of the public key recovery “rule”. The government passed the SAFE act, which regulates export of encryption keys and also requires companies to have “recovery keys” for their encryption product. This then raises the concern of protection of individual’s rights because the misuse of
these decryption keys by a tyrant leader can lead to misuse of our data and can be used to manipulate the people through constant monitoring. The government can become an all seeing, all powerful entity that can be coerced at the top and can take advantage of the technological resources to influence their will on to the people and we may not even know of this coercion. The main argument here is that the ability to use encryption keys is a form of free speech and if we would like to keep our conversation private, then we are free to do so without arising any suspicion. In the eyes of the authorities if we were to use encryption we would be giving off the perception that we have something to hide and thus bringing suspicion onto ourselves. This shows the governments intent with public recovery key, since there are people who use this technology with malicious intent. So one should ask, what are the significant harms that befall us when we do not allow privacy to be compromised? In this case, the significant harm is the intervention of the government with how we handle the privacy of our own data.

Do the benefits to public safety and other public goals of ID cards or biometrics outweigh the cost to privacy? If we could have a universal ID system where we can verify that the person is who they say they are then save billions of dollars that are lost through false identifications, wouldn’t that be a great idea? America does not require its citizens to carry ID cards on them to verify who they are. We currently have some type of identification system (ID cards or drivers license) but Some of the issues that come up and are frequently being taken advantage of by people with fake ID’s, are welfare fraud, credit card fraud, identity theft, illegal immigration, illegal gun sales and income tax fraud .We also have to worry about criminal fugitives, child abuse and sex offenders who are on the run and are using false ID’s to find jobs were they can be working with our children and elder citizens. The need to develop tamper proof identification cards is necessary to reduces some of the frauds and also to catch criminals before they get a job
working with children or elder citizens. This universal ID system would not catch all, but it would greatly reduce the number of incidents that occur every year.

The proposal of a biometric identification card that must be carried on person at all times is currently being developed and some methods are currently being employed at various government installations. All citizens are required to have this card and are required to present it when required to do so by public authorities. You are required to present this even when there is no specific evidence that a crime has been committed or a regulation violated. This brings up an issue with the violation of my privacy. If authorities were allowed to question anyone they deemed suspicious, then this would bring up concerns about racial profiling and discrimination. Universal ID is already taking place in the UK and it seems as if the government is making it mandatory for its civilians to register. If civilians don’t register their finger prints and facial scan, they can face severe fines. This proposal would meet political opposition so great that it would not be considered by U.S legislators. So a change is proposed to have those cards carry identification and medical data on them. The data would not be carried on the card; it would be located at a database. When someone would try to get more specific detail from your card, they would have to contact the database center and have to go through a process to get your information. One of the problems that come up with this mandatory ID process is the issue of denial of service if you don’t have an ID. It would create a “class of outcasts” in which individuals who do not want to use the ID system will become outcasts on the edge of society. They would be denied simple services such as daycare, school, and access to hospital emergency rooms, healthcare and so on. “allowing the government to collect and store personal medical records, and to track us as we move about in our daily lives, puts awesome power in the hands of government bureaucrats.” Whoever had access to our information has the power to invade our
privacy without us ever knowing. Our government would be rushing into a political system where the state, usually under the control of a single political organization, faction, or class domination, recognizes no limits to its authority and strives to regulate every aspect of public and private life wherever feasible; In other words, a socialist totalitarian society.

The upside to biometrics is the enhanced security features it would provide when it comes to identifying an individual. Reliable identifiers would be use to verify that the individual attempting to gain access to that information is in fact entitled to do so. Reliable identifiers could replace the use of passwords; ensure that one’s credit card is not misused, that one’s checks are not cashed by others and so on. Biometrics could go a long way toward ensuring that people are secure in their identity, thereby allowing others to trust that they are who they claim to be. But as Amitai says “although universal identifiers may diminish privacy in some respects, there is no evidence or reason to assume that their implementation will set in motion a steady descent into ever-greater restrictions on privacy and autonomy.” Meaning that even if this is implemented, it does not mean that everything will fall into place and people’s identities will be completely secured. Countries like Switzerland, Spain, France, Belgium, Germany and Portugal already employ something similar to the universal ID system and it seems like its citizens have no concerns about having to carry these ID’s, in fact many consider this normal and believe that other countries operate like this too. In fact, they could not see how anyone could not have one, since it’s the means that they use to prove who they claim to be.

Another issue that may come up is the abusive utilization of data by those that have access to it. The argument here is that there may be curious people who may want to get a snoop at someone’s personal life and start going through the database and accessing information that
they should not be entitled to. There should be methods employed to deter this from occurring and consequences to those who decide to proceed with such actions.

American society is one of the few democracies that do not have a universal ID system mainly because people feel that stepping in this direction would invade their privacy. However, the threat to us is limited since much of the information the universal ID system would have is already available in private databases and sold to all comers. The Identity Cards Act 2006 gives the Government the power to introduce ID cards in stages and the National Identity Register. While people are applying for a new passport can opt out of having an ID card, they cannot opt out of having their details recorded onto the new database. From 2010 it will be compulsory for people applying for a passport to be issued with an ID card. Our government has already taken steps in the direction of universal ID’s, so we are bound to end up with this system sooner or later. The main concern that should arise now is the possibility of our data being abused and that unreliable information about us will find its way into the system.

The thought of someone accessing our information and knowing our medical secrets is scary. “Medical privacy concerns people more than all other privacy concerns” (Amitai) Our medical information is personal and should be kept confidential between ourselves and our doctor. There has been several times where people in high trusted positions, such as medical staff who worked for Kaiser Permanente who were fined $25,000 for “snooping” at patients medical records. There have been other cases where hospital staff has disclosed medical records to insurance companies, lawyers and bankers for monetary gain. There are several corporations such as Medical Information Bureau (MIB) that maintain huge databases of people’s medical records. Whenever an individual applies for health, life or disability insurance, the company obtains the records that MIB has compiled on him/her. This
poses an issue because what the employer might learn from looking at his/her records could lead to that individual being fired. That person would have no idea that there termination was a direct result of what was learned by the employer looking at his/her medical records. There have been several reported cases where people have been fired because of “genetic discrimination” after employers learned that their employee had a serious disease. People deserve the right to keep information about their medical records private and should not be subject to losing their jobs because they are sick. People should not fear taking certain treatments just because it can go on their medical records and could possibly be used against them when filling for a job, or insurance or even a loan.

With the negative opinions that come from looking into people’s private medical records it’s hard to think that there is an upside to this; However, there are many good arguments for allowing certain individuals access to personal medical information. They play a role in ensuring public safety, improving the quality of health care, reducing costs and more importantly promoting medical research. The benefits of the aforementioned will result in better health care for all; for example, medical researchers can compare certain medical treatments and determine if it was necessary or not, create safer techniques for treatment and possibly develop new methodologies for treating certain conditions. All of this would benefit the public and possibly reduce the cost of treatment.

When applying for insurance, we have no option but to give our insurer the right to do whatever they want with our information. It’s either give in to the insurer’s demands or have no coverage whatsoever, which puts us in a very vulnerable position. What other option do we have in maintaining our medical records private? Insurers now have the right to distribute our information to employers, marketers and whomever they wish and we are allowing this to
happen by choosing coverage. The only option we have, which is out of our hands, is for the insurers to “self regulate” themselves and ensure that our private medical records are not misused or sold to other companies. I simply don’t like the idea that insurers can distribute our personal information and possibly make a profit of my privacy.

There is a war against our privacy, a war that we are slowly losing to our government. The Fourth Amendment lays out our right to privacy from government surveillance by guaranteeing that we and things we own cannot be searched or investigated without a proper warrant and probable cause. Despite this constitutionally given protection, government agents frequently trample our privacy and violate the Constitution. As Samuel D. Warren and Louis D. Brandeis noted “It was time for the common law to grow to meet the demands of society”. Our privacy is at stake and there are more laws that allow the invasion of property rather than protect it. Now is the time for command law to grow and meet our demands of simple privacy. I don’t mind my encrypted data being looked over by authorities, because I have nothing to hide and I understand that there are people that need to be dealt with and the only way to get to them, is by breaching their data, their privacy. I don’t mind having a biometric card on me, and identifying myself to authorities. If it serves to put away criminals, then it’s fine with me. I don’t mind that my medical records be used by doctors conducting research to find better ways to improve treatment and reduce costs. However, I do mind that my medical records, something I would like to keep private, is being distributed and possibly sold. I would like to see some type of government intervention in stopping these incidents from occurring. The only option I have is to not have coverage or choose coverage at the discretion that my medical information will be distributed to whom they wish; this is not a good option or solution to protecting my privacy concerning medical records. The process of finding new solutions to better protect our privacy
will be long and I hope that the wait will prove some success down the road. “Privacy is to be treated as a value that needs to be balanced with concerns for the common good.” (Amitai) The government does a descent job when it comes to providing security for the people, but it needs to understand that there is a balance that needs to be achieved between the people, before they declare that their actions is for the overall common good of the people. The fourteenth amendments provision that no state may deprive a person of life, liberty, or property without due process of law. It seems that our government has never heard of this amendment.
Works cited:


