Health Technol. (2017) 7:329–333
DOI 10.1007/s12553-017-0207-1

EDITORIAL

"Global privacy and security, by design: Turning the "privacy vs. security" paradigm on its head"

Ann Cavoukian[1]

Received: 10 July 2016 / Accepted: 26 June 2017 / Published online: 12 July 2017
© IUPESM and Springer-Verlag GmbH Germany 2017

1 Introduction

Ever since the tragic events of 9/11, and the terrorist acts that have followed, privacy has increasingly been cast as an antagonist of public safety.[1] Within the context that knowledge is power, in the last 50 years there has been a tremendous shift in the balance of power from the individual to the state – the state gathering greater knowledge of the individual while its own activities remain largely opaque to its citizens. Part of this shift has arisen from the government's ability to gain access to a much wider range of information about individuals, assisted by advances in technologies of surveillance. 9/11 has served as the rationale to collect more and more personal information (expanding the haystack) in the hopes of discovering evidence of potential terrorists (the proverbial needles). Indeed, the current surveillance paradigm that governments around the world are endorsing is to collect as much personal data as possible in the hope of enlarging the "haystack" in order to find the terrorist "needles."

Recent advances in encryption technology, however, have revamped the playing field. More secure mobile access and end-to-end encryption, is making it difficult for governments to readily access personal information at will. Governments are growing increasingly concerned about these technological trends and are calling for the creation of "backdoors" into encrypted content, that is, special "keys" reserved for them to allow unfettered access into people's encrypted communications – in other words, greater expansion of the surveillance network blanketing all individuals in society.[2]

In addition, we are witnessing massive technological changes in all things connected via the "Internet of Things," which some are calling the "Internet of Everything." While such innovation has the potential to dramatically improve our lives, it also has a dystopian side, in that it may create the opportunity for far greater subversive surveillance, which can overlay our communications and activities behind the scenes, without the knowledge or consent of those involved.

These advances in technology will also impact the state of healthcare and health research. To the extent that identifiable health data is made increasingly available through wireless and wearable health devices, without the consent of the data subjects, the privacy of potentially massive numbers of individuals will be adversely impacted. This will result in unintended consequences, not only for health research but for society at large, as medical data lands in the hands of unauthorized parties, such as one's employer or insurer.

As a result, we as a society are at a nexus. If we continue down this road of more intrusive surveillance and less privacy, we will not only become less safe as a society, but we will also become less prosperous. Respect for the privacy of all individuals in a society not only forms the bedrock of freedom, but also of innovation and its resulting prosperity. This Editorial will present that we have the technological capacity to reverse

[1] We use the term "public safety" as an all-encompassing term, which includes the necessary safety and security measures to be installed which aims to assure "a state" of public safety.

This article is part of the Topical Collection on *Privacy and Security of Medical Information*

✉ Ann Cavoukian
ann.cavoukian@ryerson.ca

[1] Privacy and Big Data Institute, Ryerson University, 350 Victoria Street, Toronto, ON M5B 2K3, Canada

[2] Abelson, Harold; "Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications", July 7, 2015, https://www.schneier.com/academic/paperfiles/paper-keys-under-doormats-CSAIL.pdf.

this ominous technological trend – that as a society we can develop systems that protect both privacy and public safety; both privacy and health research; both privacy and business interests. These are positive sum solutions which we must promote and develop, not the freedom-killing zero-sum directions of the past. "Civilization is the progress towards a society of privacy,"[3] and the loss of privacy is the regression of a society towards an uncivilized society, devoid of freedom, prosperity and ultimately of civil behavior.

But what do we mean by privacy? *There is so much misinformation about what privacy is, and is not.* Privacy is not about secrecy, it's not about having something to hide. *Privacy equals control: personal control over the uses of your personally identifiable data.* The use and disclosure of your personal information should be under your control. Decisions relating to your personal information should be made by the individual to whom the data relates (the data subject). Personal control is especially important because of context – context is key to privacy. Only the individual to whom the data relate will be aware of the unique circumstances associated with the data, and thus he/she is the only one who can truly make the determination as to whether certain data should be disclosed. This notion of personal control and freedom of choice is critical to privacy: *it is the individual, who must be free to make that determination.*

The Germans have an engaging term for this called "Informational Self-Determination": The individual must be the one who determines the fate of his or her personal information. Informational self-determination was considered to be such an important value in Germany that it was enshrined as a right in their constitution in 1983. So when you think of privacy, think about control – personal control to decide on the uses relating to one's personal information.

2 Does collection of more information on all citizens make us safer?

Governments have been fear-mongering for years, advancing the message that the "terrorist sky will be falling upon us" unless they have greater control over the ability to access more and more personal information – that in order to have public safety, we must give up some of our privacy. The reality is that most government agencies, public media and society at large, have bought into this zero-sum view of thinking. It is the prevailing view today, which is treated as a given. That is why we see public polling, which favors public safety, always at the expense of privacy. But privacy vs. public safety is a meme that has pervaded our culture because of bad information, ignorance and fear. The reality is that this view of privacy vs. public safety harms both, but more importantly, as is discussed below, it jeopardizes our prosperity as a nation.

The premise underlying the government's message is that more data translates to greater public safety – but the evidence suggests otherwise. The failure to stop terrorist attacks, from 9/11 to the present-day San Bernardino/Brussels/Orlando attacks, has not been the consequence of too little information; it has been the consequence of not connecting the dots with the existing information that law enforcement and intelligence agencies had acquired, and was already in their possession, through legitimate means. Days before the Brussels terrorist attack, officials from Paris intelligence alerted law enforcement officials in Brussels as to a number of distressing emails they had accessed, relating to a possible terrorist attack in Brussels in the days to come. This information was regrettably not acted upon.

The evidence suggests that governments largely possess the means to prevent such attacks, using tried and true techniques – if they focus on using and sharing the information they already possess more effectively, without violating individual privacy or mandating insecure encryption. The latter will only serve to strip law-abiding citizens of their privacy and the security of their online communications and transactions.

Further, the rationale that broad fishing expeditions to collect personal data (enlarge the "haystack") increases the probability of finding terrorist "needles" is patently false and mathematically specious. The reason is that with the vast amounts of data being collected, even an army of humans could not sift through all the data to discover the "potential needles." Therefore, machine learning techniques that classify data into classes must be turned to. The methodology is to use a training set of examples comprising the data collected (activities and events such as GPS location, web browsing, credit card transactions, telephone metadata, etc.) and the target classes (potential terrorist or innocent individual) to learn a model that hopefully will correctly classify new examples, not seen before. The goal of the machine learning algorithm, however, is not to memorize the training set, but to use the training set to learn how to generalize to novel inputs (a new set of data on an unknown class of individual). But there is always a tradeoff: perfect accuracy can never be achieved; therefore one has to tradeoff between false negatives (a terrorist is missed) and false positives (an innocent individual is falsely tagged). There will always be errors associated with the classification of data. The magnitude of the error will be a function of the type and complexity of the algorithmic model, and most importantly, the amount of training data – the more training data that is available, the greater the model complexity tolerable before over-fitting. However, regardless of how optimum the foregoing may be, there will always be errors.

As an example, the **Skynet** surveillance program in Pakistan which looks at telephone metadata to target terrorists for potential drone strikes uses the Random Forest machine learning algorithm. As a tradeoff, they set the false negatives at a high

[3] Ayn Rand; "The Fountainhead," New American Library, New York, NY, 2016

value of 50% in order to decrease the false positives (in this case, meaning not killing innocent people). The false positive rate was set at 0.18%.[4] If the false negative rate was lowered below 50%, the false positive rate would escalate accordingly. That is the manner in which these algorithms work.

Now, assume that this false positive rate of 0.18% was applied to North America. That would mean that for every one hundred million people, there would be 180,000 false positives – innocent people being tagged, with 50% of the "bad guys" being missed. That would mean that for all of North America, there would literally be hundreds of thousands of false alarms, which in most cases, would need to be handled manually, resulting in a staggering cost in human resources. Most false positives would need to be investigated because one can never know beforehand whether they are indeed false because some real terrorists may be mixed in with them. So in fact, security will become far worse in the attempt to find the actual needles, not better, as uninformed politicians seem to be suggesting. This is not enhancing public safety. Law enforcement resources must be used, and in effect wasted, in order to filter through the many false positives, based on the billions of data records collected.

However, we believe that Machine Learning experts working for the NSA, for example, understand these issues and are not in fact using collected data to search for needles. So why are they collecting all of this data? What it does allow is for Intelligence agencies and law enforcement to query their databases on the past activities of actual suspects, and to flag all of their future activities. In this case, in order to query the database, the identity of the individual must be known beforehand in some fashion such as their name, address, social security number or a credit card number, etc. These suspects may be potential terrorists and criminals, but what is disturbing is that they may also be individuals who do not tow the current party-line such as reporters, demonstrators, union leaders, "radicals" and so forth.

The argument government uses is that they can now issue a warrant to target specific individuals in the database, whereas in the past, a warrant would not necessarily provide access to past activities which were not collected. This new protocol effectively castrates the American Constitution's Fourth Amendment rights, in its attempt to protect individuals from an overbearing government. Privacy is clearly harmed since more and more of an individual's activities are gathered, recorded and monitored without the necessary probable cause/warrant rationale. But also, public safety may be harmed since in trying to balance against privacy, the necessary steps and precautions to protect society may not be taken in the name of privacy, in which case, zero-sum harms both privacy and security.

[4] Christian Grothoff & J.M. Porup; "The NSA's SKYNET program may be killing thousands of innocent people: "Ridiculously optimistic" machine learning algorithm is "completely bullshit," says expert," arsTECHNICA (UK), 16 February 2016 .

With respect to the question of creating backdoors to means and methods of encryption, in theory this would give law enforcement the ability to access encrypted data, whereas before, the protection offered by encryption would make this impossible. However, contrary to what the proponents of back-doors may believe, the reality is very different. What is obvious to all cryptographers and security experts is that you cannot build a "back-door" which only the "good guys" can access. The "bad guys" will quickly discover these additional points of access and will indeed gain entry. You only need to look at the spate of hacks and data breaches reported on a daily basis to understand the difficulty of maintaining strong data security, even without the handicap of a government-imposed insecure backdoor.

Moreover, from a practical perspective, the majority of data infrastructure is now protected by strong encryption. Do we really think that businesses are going to "trade-in" their "good" security for the "bad" security that governments want us to have? Encryption is essential to preserving security in an insecure Internet. Any web site which uses "https:" uses encryption with which to communicate securely. This enables the secure transfer of passwords, credit card numbers, mobile payments, etc. and allows you to shop on Cyber Monday without the fear of identity theft. Encryption protects your medical records, your banking records, your financial transactions, and permits you to securely file your taxes online. This is only a fraction of the security it provides throughout the entire networked infrastructure of the Internet.

But encryption serves a far broader purpose than facilitating security: it enables our very freedom in a digital world. Encryption is a vital tool for enabling journalists to operate in countries without freedom of the press; it allows dissidents to coordinate against oppressive regimes, and in democracies, encryption empowers ordinary citizens to counteract intrusive government surveillance programs.

Despite these facts, the view commonly held is that privacy is the polar opposite of public safety or business interests, whose enhancement undercuts the effectiveness of the latter two objectives. And unfortunately, this is one of the most damaging paradigms in existence in the present-day cyber age. This zero-sum, win/lose paradigm of privacy vs. public safety is not only wrong, it is extremely dangerous, and must be brought to an end. It is wrong, because privacy and public safety can indeed co-exist, resulting in greater efficacy for both. It is dangerous because in the tension between privacy and public safety, privacy will always lose, and this loss will directly endanger not only freedom, but the prosperity that we enjoy as a free and open society.

3 Privacy and prosperity

In the last century, we have enjoyed tremendous prosperity, arising from massive innovation. It was thought that this

prosperity arose as a result of unencumbered freedom and the absence of onerous regulations on innovators. But this prosperity was also a result of privacy and minimal levels of surveillance. Prior to the 1980's, today's technologies of mass surveillance had largely not been invented. An individual's privacy was for the most part secured by default – often through practical obscurity. But since then, the technologies developed have lent themselves to assisting surveillance on a considerable scale. And the type of surveillance developed targeted not only terrorists and criminals but all individuals, including law-abiding citizens.

Privacy is essential to society, at so many levels: privacy is at the root of both freedom and prosperity. It is the prosperity of a society that allows the products of innovation to be shared by all members, including those in the lower socio-economic strata. Smartphones, for example, enhance the lives of both the rich and the poor, but perhaps even more important, innovations in transportation, healthcare, the arts, smart appliances and communications are enjoyed by all, making our quality of life far better than that of our parents and grandparents, only a few generations earlier. Innovation is what makes it all happen – but what makes innovation happen? Just look around the world. The most innovative societies also happen to be the most free and privacy protective. Freedom and privacy form the foundation, the very bedrock, of all innovation. Compare the progress, or lack thereof, between East Germany (before the wall came down), and West Germany: the latter was highly successful, both economically and creatively, regarding innovative developments, compared to their repressed counterpart of East Germany.

4 How is privacy connected to innovation?

Innovation requires taking risks and being able to think differently, at times contrary to the existing memes prevalent in a given culture. And at times, this may require being on the "edge," or perhaps even going over the edge – thinking far outside of the box, so to speak. It requires that an individual's mind shed any barriers to imagination, either self or externally imposed, because innovations arise from the very crystallization of that imagination. Accordingly, we want to enable wild and sometimes crazy imaginative ideas, ideas that may initially fail, but with greater effort, become the future products of innovation, for both commerce and the arts.

But if one is constantly being watched – continuously surveilled, and all of one's activities are monitored and stored for future data mining and assessment, or perhaps to establish a profile of of a person, of one's life, or one's edgy predilections (even though lawful), then in effect, consciously or subconsciously, one will focus on being watched, and instinctively will modify one's behaviour. But it goes much further than that.

The government through its warnings to be vigilant about potential terrorist acts, and the media broadcasting constant reminders that things are getting worse, and "talking heads" arguing that we need to give up "some" of our privacy, instills yet more fear and anxiety in society. This is compounded by the government saying that in order to prevent us from getting potentially "blown up," they must surveil our activities even more. This could be viewed as an oppressive act, which would effectively restrict one's freedoms. Under such conditions, our cognitive processing will be limited to, at best, a few contexts associated with anxiety and most likely fear. We will be less likely to be able to draw upon contexts which may lead to creative imagination and innovation. The reason for this is due to our subconscious, which greatly influences our conscious experience of thoughts and reality – in this case, a reality which relates to the anxiety of knowing that we are constantly being watched, while at the same time, fearful of being in danger of being blown up. This is one of the unfortunate consequences of the state we are in and the surveillance that it engenders. The tragic outcomes from practices of The Ministry of State Security (Stasi), of East Germany, was a vast psychological experiment, which provided strong evidence of the above fact (resulting in present-day unified Germany becoming the leading privacy and data protection country in the world, saying "never again").

Human beings evolved to be wary of the watchers, and that behaviour in humans, in direct response to such surveillance, inhibits the ability to allow our imaginations to soar and enter the vistas of true creativity and innovation. There will be individual differences no doubt, but it would not be an overstatement to say that some of the most creative and innovative individuals in society are also those who would be the most susceptible to the anxiety of constant surveillance. As a result, if states of surveillance persist, the level of innovation as a society would be expected to drop considerably over the next generation. Privacy means that one is free to voluntarily expose one's thoughts and activities, as one so chooses, in whatever areas one wishes. And as such, one is free still retain the open vistas of one's mind – there is no fear or anxiety which serves to limit the cognitive bandwidth, leaving one open to potentially imagine ideas that extend well beyond the current reality.

However, what about security and public safety, you ask? Don't we have to give up some privacy in order to remain safe? No, this is precisely the overbearing paradigm that will ultimately destroy all freedom and prosperity in our society, and the overwhelming tragedy is that it is false. We can have public safety, security, privacy and freedom without sacrificing or needing to "balance" one of these interests against another. It is ludicrous to think that a society of innovators cannot develop systems that protect both public safety and privacy. (See paper on Operationalizing Privacy by Design[5]). Such is the type of

[5] Cavoukian, Ann; "Operationalizing Privacy by Design: A Guide to Implementing Strong Privacy Practices," Information & Privacy Commissioner of Ontario, Canada, December, 2012. http://www.ontla.on.ca/library/repository/mon/26012/320220.pdf

thinking that arises from a perspective of fear. It results in accepting the *status quo* of ignorance.

If we are to survive as a free and prosperous society, we must replace the zero-sum meme with positive-sum messaging, which will allow us to be serious about building innovative systems that integrate both privacy and public safety, without either being compromised, allowing us to achieve doubly-enabling solutions. This mind shift in society can only be accomplished through massive education and raising of awareness. It rests in the design of the systems and the technologies that we put into place. The former represents a win/lose, zero-sum paradigm – privacy vs. public safety that, over time, degenerates into a negative sum, lose/lose proposition. The latter represents a win/win, positive-sum framework, wherein the interests of both privacy and public safety may be reflected.

5 The challenge

Let there be no mistake: privacy is a necessary condition for both a prosperous and free society and overcoming this zero-sum paradigm is the only solution to future prosperity in a digital age. The remedy is a positive-sum, win/win model where relevant systems are designed with both objectives in mind. 10 years ago, this author introduced the critical concept of "*Privacy by Design.*" However, the fear of terrorism, as tangible as it is, is overtaking the dissemination of the message that we can have both privacy AND public safety, without sacrificing the efficacy of one for the other.

Therefore, we must expand our efforts beyond the original purpose of "*Privacy by Design,*" which was primarily education by a limited number of privacy advocates. It is necessary for the majority of individuals who value freedom, privacy, prosperity and public safety to join a movement in spreading the message that we as a society have the innovative ability to build systems that protect both privacy and public safety while allowing business interests to flourish. This will require technologists to think outside of the box – to develop methods that will deliver both privacy and public safety; privacy and data analytics. Likewise, policy-makers, lawyers, and politicians – anyone interested in preserving our freedoms and prosperity, must join to reorient and to redirect our attention, our focus and action.

As freedom-loving societies, we must dispel the commonly held view, held by governments, businesses, the media and the public at large – that one must choose between privacy and public safety. Our goal is threefold: First, to educate politicians, businesses, the media and public that we can and must engineer systems to protect both privacy, and other interests. We can do this by, for example, using innovative technologies such as recently developed advances in Artificial Intelligence and Machine Learning, Blockchain and Homomorphic encryption. We must do this because the loss of privacy to surveillance will not only undercut our freedoms, but the prosperity resulting from a society of innovators. Accordingly, our second goal is to foster technology innovation in academic institutions around the world that will allow privacy and public safety, as well as privacy and business interests such as Big Data and data analytics, to be achieved without sacrificing either. Third, we wish to develop policy templates which will articulate how privacy is to be applied in the new digital age for different government and business segments, and the oversight these institutions should fall under. These policy templates will be important in the development of new, doubly-enabling, positive-sum technologies.

If we intend to preserve our freedoms, now and well into the future, we must embrace both privacy and security, ***in unison, and by design.*** In this day and age of growing fears over terrorist attacks, we cannot forfeit our privacy, and in turn our freedom and prosperity, to these amplified fears. We must demonstrate that we can indeed have both privacy and public safety, otherwise our freedom and prosperity will be forfeited, which in our view, is simply too high a price to pay.

Compliance with ethical standards

Conflict of interest The author declares no conflict of interest.

Funding There is no funding source for this article.

Ethical approval This article does not contain any data, or other information from studies or experimentation, with the involvement of human or animal subjects.