©CREATIVE COMMONS/ XYAN BHATNAGAR

International council on global privacy and security, by design

By Ann Cavoukian

©ISTOCKPHOTO.COM/ARCHERIX

Make no mistake, privacy is a necessary condition for both a prosperous and free society. However, ever since the tragic events of 11 September 2001 and the terrorist acts that have followed, privacy has been increasingly cast as an antagonist of public safety. (I use the term *public safety* as an all-encompassing term that includes the necessary security measures to bring it about.) This zero-sum, win/lose paradigm of privacy versus 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 coexist, 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.

The remedy to overcoming this zero-sum paradigm is a positive-sum, win/win model, where relevant systems are designed with both objectives in mind. I started this process well over ten years ago by introducing the 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, I believe we must expand our efforts relating to the exposure of the messaging of Privacy by Design. So, I am asking those of you who value freedom, privacy, prosperity, security, and public safety to join me in spreading the word—that you can indeed have privacy *and* functionality. I ask technologists to join me in thinking outside the box—to develop methods that will deliver both privacy and public safety; privacy and data analytics. Likewise, I ask policy-makers, lawyers, and politicians—anyone interested in preserving our freedoms and prosperity—to join us in this endeavor. The vehicle for this nascent movement is the newly created International Council on Global Privacy and Security, by Design (GPS by Design), which, by necessity, must be international in nature since data no longer resides within one's borders.

The Mission of GPS by Design is to dispel the commonly held view—held by governments, businesses, the media, and the public at large—that one must choose between

Digital Object Identifier 10.1109/MPOT.2016.2569741
Date of publication: 8 September 2016

0278-6648/16©2016IEEE

privacy and public safety. Our goal is threefold: First, to educate politicians, businesses, the media, and the public that we can and must engineer systems to protect both privacy and other interests. We can do this by using, for example, innovative technologies, such as recently developed advances in artificial intelligence, 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.

"Civilization is the progress towards a society of privacy," wrote Ayn Rand, in *The Fountainhead*, and the loss of privacy is the regression of a society toward an uncivilized society, lacking in freedom. 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 that will articulate how privacy is to be applied in the new digital age for different government and business segments and the oversight under which these institutions should fall. These policy templates will be important in the development of new, doubly enabling, positive-sum technologies.

This is a call to action: We are seeking to enlist the support of like-minded people from around the world who will commit to spreading this message. (Privacy by Design has already achieved a true global presence, having been translated into 38 languages, so our intention is to leverage off of this status.) 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 escalating fears. We must demonstrate that we can have both privacy and public safety, otherwise our freedom and prosperity will be forfeited, which is simply too high a price to pay.

Cavoukian, who is the former Information and Privacy commissioner of Ontario, Canada, currently serves as the executive director of the Privacy and Big Data Institute at Ryerson University.

The Mission of GPS by Design is to dispel the commonly held view that one must choose between privacy and public safety.

A seismic shift

There has been a tremendous shift in the balance of power from the individual to the state. Part of this shift has been the government's ability to access a wide range of information about individuals. In the last 40 years, this access has been greatly assisted by advances in technology. But now, because of new technology, this balance of power has a chance of shifting back toward the individual. As a result, governments are growing increasingly concerned and want to prevent this from happening.

Encryption technology has now revamped the playing field, wherein governments can no longer readily access personal information at will, as a result of end-to-end encryption. This, in turn, has led to calls by law enforcement for the creation of "backdoors" into encrypted content, which can lead to far greater surveillance. In addition, the introduction of the Internet of Things will create the opportunity for even more subversive surveillance that will widely blanket society.

As a result, we as a society are at a nexus. Governments have been fear-mongering, essentially saying that the "terrorist sky will fall upon us" unless they have complete control and access to more personal information. But the evidence suggests otherwise. The failure to stop terrorist attacks, from 9/11 to the present-day San Bernandino/Brussels 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 already acquired and was in their possession through legitimate means. The evidence suggests that governments largely possess the means to prevent such attacks using tried and true techniques and, 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.

Despite these facts, the commonly held view is that privacy is the polar opposite of public safety or business interests, whose enhancement undercuts the effectiveness of the latter two objectives. This is referred to as a *zero-sum game*, whose either/or, win/lose tension can only be addressed by the victory of one objective, always to the detriment of the other. Unfortunately, this is one of the most damaging paradigms in existence in the present-day cyber age. It will directly detract from our prosperity and freedom as a society.

Looking back

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 1980s, today's technologies of 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 grand scale. The type of surveillance developed targeted not only terrorists and criminals but all individuals, including law-abiding citizens.

Our argument is that 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, health care, 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 innovation.

So what is the connection to privacy?

Innovation requires taking risks and being able to think differently, at times contrary to the existing memes prevalent in a given culture. At times, this may require being on the "edge," or perhaps even going over the edge—thinking far outside 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.

If I am constantly being watched—continuously surveilled, and all of my activities are monitored and stored for future data mining and assessment, or perhaps to establish a profile of me, of my life, or my edgy predilections (even though lawful)—then in effect, consciously or subconsciously, I will focus on being watched, and instinctively, I will modify my behavior. 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, with "talking heads" arguing that we need to give up "some" of our privacy, instill yet more fear and anxiety in society. This is compounded by the government saying that to prevent us from getting potentially "blown up," they must watch and surveil our activities even more. 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 that may lead to creative imagination and innovation. The reason for this is largely due to our subconscious, which greatly influences our conscious experience of thoughts and reality—in this case, a reality that relates to the anxiety of knowing that we are constantly being watched while, at the same time, fearful of being in danger of getting blown up. This is one of the unfortunate consequences of the state we are in and the surveillance that it engenders. The tragedy of Stasi Germany was a vast psychological experiment that provided strong evidence of this fact (resulting in present-day Germany becoming the leading privacy and data protection country in the world, saying "never again").

We evolved to be wary of the watchers, and that behavior 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.

We evolved to be wary of the watchers, and that behavior 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 we believe that the level of innovation as a society will drop considerably over the next generation as a result. Privacy means that I am free to voluntarily expose my thoughts and activities as I so choose in whatever areas I wish. As such, I still retain the open vistas of my mind—there is no fear or anxiety that serves to limit my cognitive bandwidth, leaving me open to imagine ideas that potentially extend well beyond the current reality.

Privacy and public safety

But what about security and public safety? Don't we have to give up some privacy 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 the paper on Operationalizing Privacy by Design (Cavoukian, 2012)]. This is the type of thinking that arises from a perspective of fear. It results in accepting the status quo of ignorance.

We need not give up on privacy, we simply need to embed it in design, along with security.

Unfortunately, the reality is that most government agencies, public media, and society have bought into this zero-sum view of thinking. It is the prevailing view held by most governments, politicians, and businesses alike, being treated as a given. That is why we see public polling that favors public safety, always at the expense of privacy. But privacy versus public safety is not a fact of reality; it is a meme that has pervaded our culture because of bad information, ignorance, and, especially, fear. The reality is that this view of privacy versus public safety harms both.

For example, law enforcement and intelligence agencies engage in broad fishing expeditions in an attempt to find the needle in the haystack while creating a trove of false positives. This is not effective public safety because law enforcement resources must be used, and, in effect, wasted, to filter through millions of false positives based on the billions of data records collected. Privacy is clearly harmed since more of an individual’s activities may be monitored without the necessary probable cause/warrant rationale. But also, in some cases, public safety is harmed since, in trying to balance against privacy, the necessary steps and precautions to protect society may not be taken, all in the name of privacy, in which case, zero-sum harms both privacy and security.

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 one 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 versus 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.

The challenge

The zero-sum paradigm is the view that we wish to dispel, and those joining our council will commit to doing so. In my previous role as Information and Privacy commissioner of the Canadian province of Ontario, we demonstrated countless ways in which this could be achieved, leading to positive, win/win outcomes. This was accomplished through a framework called Privacy by Design, which seeks to proactively embed privacy protective measures into the design of information technologies, networked infrastructure, and business practices in an effort to prevent privacy harms and data breaches from arising.

Privacy by Design is a model of prevention, before the fact: by identifying potential risks proactively, you may then embed the necessary measures into programs and IT to prevent the harms from arising—bake privacy-protective measures into the code, into the data architecture, resulting in positive-sum, win/win solutions. A key step is strong security, which is featured as an essential component: while privacy subsumes a much broader set of protections than security alone, if you don’t lead with strong security, end-to-end, with full lifecycle protection, you will never have good privacy.

Privacy revolves around personal control over one’s data. We must have both privacy and security in equal measure. We need not give up on privacy, we simply need to embed it in design along with security. We invite you to join our international council to help bring this about: here’s to the end of zero-sum paradigms and a future filled with privacy, security, freedom, innovation, and prosperity!

Read more about it

- A. Cavoukian, “Operationalizing Privacy by Design,” Ontario, Canada, 2012.

About the author

Ann Cavoukian (ann.cavoukian@gpsbydesign.org) is recognized as one of the world’s leading privacy experts. She is presently the executive director of the Privacy and Big Data Institute at Ryerson University, Toronto, Canada. She served an unprecedented three terms as the Information and Privacy commissioner of Ontario, where she created Privacy by Design—a framework that seeks to proactively embed privacy into the design of information technology and networked infrastructure, thereby achieving the strongest protections possible.