Prologue by Evan Wolff

Partner in Crowell & Moring.

watch video

Current global policy debates highlight the tension between cybersecurity, with its emphasis on increased information monitoring and sharing, and privacy, with its expectation that personal information will be protected above all else.

Trust, from three different perspectives, is the key to reducing this tension and harmonizing cybersecurity needs with privacy expectations.

First, individuals must trust technology and custodians of personal information not only to protect their data but also to provide solutions when things go wrong. That trust arises from custodians being transparent about how electronic information is collected, secured, used, shared, and disposed of.

Second, businesses must trust information security systems and related controls to provide reasonable, risk-based protection for their intellectual property and business data and their customers' and business partners' data. Businesses also need to trust technology to be sufficiently robust and flexible to comply with an evolving array of government regulation, information sharing initiatives, and privacy requirements.

Third, nations must trust that the cybersecurity technology, policies, and practices upon which they rely will be sufficient to defend their electronic borders against cyber threats, while also protecting the data of their citizens and businesses in a manner that strikes a reasonable balance between national security and law enforcement needs and citizen's privacy expectations.

Cybersecurity technology, tools, and policies are critical for protecting information and physical security, just as privacy laws and policies are necessary for protecting personal information. Trust that cybersecurity and privacy can not only co-exist but also complement each other will develop with discussions about the intersection of cybersecurity and privacy, the challenges that cybersecurity and privacy pose for each other, and the importance to each of transparency and accountability.

Intimacy and privacy versus cybersecurity

2.3

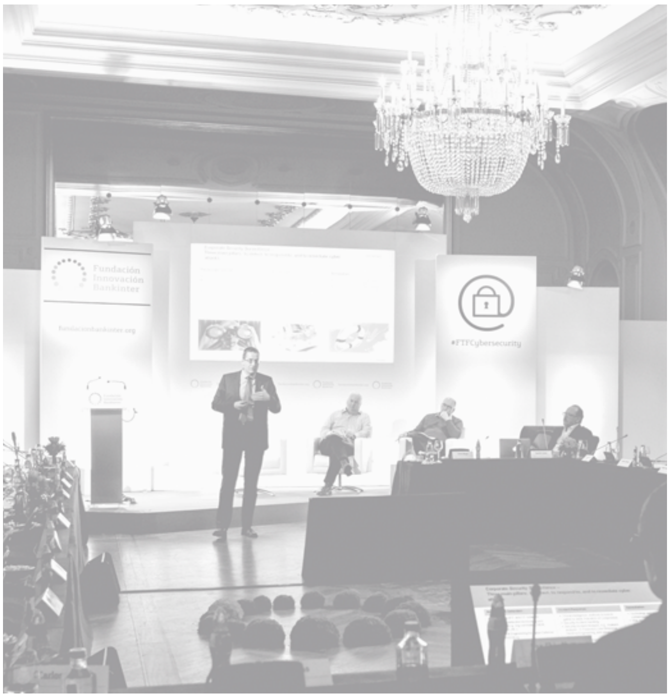
Since the controversial revelations of Edward Snowden in 2013, the public have known that world governments have a serious interest in having access to all the data that circulate on the internet. The former computer engineer at the National Security Agency (NSA) https://www.nsa.gov/ uncovered unethical practices by the U.S. Government and its "Prism" program, which used 0-day or "zero day" vulnerabilities to monitor certain sectors of the population.

Would the loss of privacy with the aim of supposedly achieving citizen security be justified in modern societies?

One of the five settings of society that the experts worked on was precisely a system that is completely controlled by the Government. From a technological point of view, this is a possible situation in the new era of the Internet thanks to the widespread existence of systems and sensors at a low price, which would make it a possibility in some countries, especially after a massive terrorist attack that would send the population into a panic. The conclusion of a model like this is that there would be no privacy and people would end up suffering from mental disorders.

On the other hand, according to experts, guaranteeing security in a world where privacy is above everything would be complicated, because data would always be encrypted so it cannot be revealed, including any communications between terrorist. Nonetheless, individuals would have control of their data and their privacy would be safeguarded. The experts warn that cyber felons would tend to abuse the easy access to all types information on the Internet.

"I really do not believe in privacy on the Internet. I believe that we need a stricter authentication for Internet privacy and security when necessary, but when it is not required, anonymity should prevail", explains **Evan Wolff**, a partner at Crowell & Moring (watch video). The citizens are currently at a disadvantage in cyberspace and felons have an advantage over them, he insists. Why? , he wonders. Managing digital identification is very complicated and managing authentication even more. Authenticating somebody in cyberspace



By 2020, he predicts that the cycles of threat detection will be reduced in companies with the use of more predictive systems and intelligent security analytics.

and verifying that the digital and real identities of a person match has become a very complicated task, whereas maintaining a user's anonymity is "very, very easy", he adds. For example, "WhatsApp", the popular communications service, hardly requests any details to register.

The expert is confident that the upcoming quantum leap in technology programming and innovation will be decisive in improving authentication systems and defining concepts about privacy that benefit the digital citizens.

As a result, they will be more protected against cyber felons. He also expects that countries and large companies will start to organise themselves to work together towards these objectives.

One of his predictions for 2020 is that companies will be more transparent with respect to what they do with their customers' data, and this will contribute to guaranteeing their privacy. Regulations will be part of the process, but they will not be decisive, because these things do not work by enforcing legislation, he points out.

From the business sector, **Rolf Reinema**, of Siemens, assures that "we have to find a suitable balance between the necessary control of security and preserving privacy. Usually, the tendency is to compile everything and then analyse it. This has some negative privacy implications, because the data collected by companies to prevent cyberattacks could also be used for other intentions.

The use of personal data by companies

Some companies work with very powerful threat detection and monitoring tools, but there are still vulnerabilities in their infrastructures. The processing of millions of data in real time or Big Data is now possible thanks to current computers being increasingly smarter, and they also allow defining behavioural patterns, trends and guidelines of cyber felons, as well as predicting possible threats from data analysis.

In the same way that governments monitor citizens under the argument of security, companies tend to collect all possible data with the purpose of subsequently deciding which could be useful, says Reinema. "We must make sure that these data is not used inappropriately. We focus on the collection of data, but many times, we do not concentrate on protecting them. And these data could be interesting for others", according to Reinema.

The citizen does nothing; technology takes care of guaranteeing his security.

By 2020, he predicts that the cycles of threat detection will be reduced in companies with the use of more predictive systems and intelligent security analytics, which in the event of cyberthreats will trigger alarms much earlier than now. This will provide companies with real-time cybersecurity indicators, and it will expedite the mitigation of attacks.

With regard to these issues, "the stupidity" that one sometimes detects is unbelievable, warns Michael Schrage, of the MIT Center for Digital Business. On the one hand, we demand security, but paradoxically, on the other, our privacy cannot be violated, he adds. The question has nothing to do with legislating or not, but with the inherent conflicts between regulations that compete with each other to fulfil their own objectives and with the purpose of guaranteeing a security that, in some way or another "does not infect or contaminate other assets." This, by itself, "is not only naive but also a mirage", he specifies.

Does technology change the behaviour of people? Which would be the best way of promoting privacy and security? Through new technology solutions or by encouraging different behaviours? The majority defends the combination of several measures as the key to success. The solution would have to involve the search for a balance between legislation, social and educational awareness, innovative technology, etc.

Regulations are important, maintains the deputy chairman of Constellation Research, **Steve Wilson**. Although some countries disagree, "of course laws change the behaviour of people in the very long term", he assures. To justify his arguments, he points to the compulsory

Michael Schrage ▾
Research fellow, MIT Center for Digital Business.

The solution would have to involve the search for a balance between legislation, social and educational awareness, innovative technology, etc.

use of seat belts in vehicles as an example, which was highly successful in guaranteeing the security in the automotive industry.

Michael Schrage, of the MIT, says that technology by itself is much more effective than any law that seeks to impose certain behaviours, even in terms of personal security. He proves this by presenting the example of the airbags used in cars to protect passengers in the event of an accident. He explains that the user does not have to remember whether to activate it or not, because it works automatically when needed. The citizen does nothing; technology takes care of guaranteeing his security.

He even adds that certain small defects in the architecture of technologies, intentionally built in by its developers to activate from time to time, would undoubtedly guarantee the security or privacy of the user much more effectively than many recommendations or laws.

If we ask someone, for example, to memorise a new password every six weeks in order to protect his identity on the Internet, it probably will not be so effective as the activation of some type of mechanism in the system that from time to time automatically encrypts the user's passwords in order to force him to set new ones for security reasons, he adds.

The book "Nudge" by professors Richard H. Thaler and Cass R. Sunstein, specifically explains that you can help people to make important decisions in their life by slightly pushing or nudging them to do so, as exemplified by the aforementioned case of encrypting passwords from time to time with the purpose of forcing users, in a nice way, to change them.

John Lyons, of ICSPA, makes good use of the debate to highlight the importance of privacy on the Internet not only for citizens but also for companies, whose significance should not be underestimated under the argument of having to give preference to other requirements such as security, which, of course, is also important. He warns that South American countries or some Asian countries, among others, could prefer technological products and the innovation produced by certain geographical areas in the world, such as Europe, instead of others, because they guarantee a further commitment to privacy in their products and services.

“I really do not believe in privacy on the Internet. I believe that we need a stricter authentication for Internet privacy and security when necessary, but when it is not required, anonymity should prevail”

Evan Wolff

Partner in Crowell & Moring.