feature

Privacy in the Era of Monitoring and Surveillance

A Conceptual Framework on Personal Data Protection

Many believe this is a period in human history in which geopolitical tensions perpetuate uncertainty, doubts and fear. It is not possible to foresee the actions of countries or clearly determine their intentions. The world is living in a state of tense peace where, in some way, everyone observes one another in an effort to understand and anticipate what might happen and not to be caught off guard.

The need to know is overwhelming for those who are not capable of examining and forecasting the next steps of their key competitors. It is a disadvantage to be at the mercy of other intelligence systems and even worse to be stripped of strategic and competitive advantages in any business sector. In this situation, thinking of security, control or privacy of information gives rise to a contradictory and challenging paradigm regarding the reaction to a reality that seeks to disclose and implicate.

Within this framework, privacy is threatened due to its coexistence as an ally of the people and, especially, as a right of individuals in the midst of a monitoring and surveillance society. As more technology is embraced and integrated into products and services,[1] there is increased flow of information and, therefore, a higher probability that personal information will be compromised.

In light of this, it is important to review in detail some elements that cause adverse effects to privacy. It is also necessary to establish a privacy protection model that not only takes into account a nation's laws and practices, but that also includes organizations' current security and control practices, as well as people's behavior, as a key alternative to other models in the midst of international tensions.

Jeimy J. Cano, Ph.D., CFC, CFE, CMAS
Is a research member of the Grupo de Estudios en Comercio Electrónico, Telecomunicaciones e Informática (GECTI) of the law school and a distinguished professor at the Universidad de los Andes (Bogota, Colombia). He has been a practitioner and researcher on information security, data privacy, information technologies and digital forensic science for more than 20 years working in different industries. He was a member of ISACA's Publications Subcommittee. Cano can be reached at *jjcano@yahoo.com.*

Elements That Generate Tension in the Protection of Personal Data

Among the key elements that must be reviewed are the influence and control of developed countries with the highest concentration of multinational companies and technological advances that permeate businesses and the needs of the people. These countries must seek positive, large-scale alternatives for their businesses to strengthen their financial activities and maintain flows of capital that encourage emerging markets.

Another factor in this controversial reality is national regulations that bring about tension and cause actions that protect the expectations and realities of individual countries with respect to the protection of their own interests. These interests are often negotiated and encouraged by economic agreements that allow the flow of investments and information that promote win-win alliances in which products and services are aligned with standards set by entities, many of which are located in developed countries.

Another element to be considered is understanding privacy. In English-speaking countries, this is usually a paid service confirmed through commercial agreements; however, in Central European countries, it is a right for which implementation and compliance are delegated to the state. Both positions have some issues. The first is motivated by commercial and business forces and the second is focused on the person and its implications as a constitutional right.

If these three elements are placed in the current scenario of monitoring and surveillance, the questions to ask are: What will the priority be when implementing the protection of personal information or when considering national needs, aided by the protection of the state, as an invaluable asset? What will the priority be when considering the commercial needs of a global world or the recognition of the

individual from the point of view of the dignity that stems from a constitutional right?

Whatever the answer, tension will be present. The exercise of protecting personal information requires concessions to be made regarding any of the analyzed aspects. In this regard, the question for the individual is: For which product or service would you be willing to share your personal information? In other words, would you be willing to give up your privacy, to waive the right to not reveal something personal that distinguishes and identifies you?

New Standards for the Protection of Personal Information

We are living in a new computing and industrial revolution that questions the current conditions of the prevailing technological developments. The increasingly urgent need to obtain information to make decisions and explore future opportunities[2] creates a scenario in which information must be instantaneous (on social networks), on the move, in the cloud, analyzed and connected to the reality of things.

In this context, trying to contain or maintain information that should be withheld, whether due to business conditions or regulatory compliance, is becoming an even greater challenge as almost everything invites and suggests a connection or transmission of information. This implies a decision that, in the end, is in the hands of the individuals who have access to it, subject to their security and control criteria as well as their understanding of the protection of personal information.[3]

Accordingly, there are several considerations that must be analyzed with regard to the transparency of organizations in a world of asymmetrical information.[4] As mentioned in the personal information scenario, these are of interest given the understanding of the interconnected reality and the need to know and share demanded by a society of information and knowledge.

The considerations mentioned are:

- **Review assumptions on how to keep information secure.** Keeping secrets or establishing limits to information access will continue to become more complicated and more demanding. These efforts may be successful at times and not at others. Regarding personal information, practices related to accessing personal information, its continuous validation and the appropriation of the risk that this information means for organizations are elements that should be part of the governance and management of privacy for companies in this new millennium.

> **“The exercise of protecting personal information requires concessions.”**

- **Review corporate strategy regarding the undesired disclosure of information.** If the corporate strategy depends on information and its flow in management processes (i.e., it is constantly used and addressed by people in the company), it is necessary to review security and control diagrams to reduce the probability of undesired leaks of key information. Regarding personal information, classification of information, and the security and control measures associated with the sensitivity level, the protection of such information must be the base standard. Even though much of this information is continuously consulted, any unexpected leak can compromise the reliability of the company within its business environment.
- **Review operations and those issues that could be problematic if disclosed.** This is not to say that companies are hiding inappropriate things and the like, rather that companies must adjust

their processes along the entire supply chain to establish best practices that guarantee due care by the organization regarding operations and accountability to the executive team. As to personal information, the supply chain must be familiar with its flows of personal information, the best practices to be implemented, the records to be kept and the reports to be issued. A personal information breach generally motivates administrative and judicial actions against the company that experienced the security and control failure.

- **Assume that people can reveal information about an organization for their own personal reasons and that organizations cannot prevent such revelations.** This consideration refers to the management and control of the company's image. Organizations must be prepared to respond quickly, especially when the information published is incorrect. It is obvious that companies will not be able to stop intentional falsehoods disseminated through social networks, but what they can do is to record correct information in cyberspace through responsible people with facts that can be verified. If companies make public the truth about personal information issues, then those who have misappropriated data will recognize that there will be risk and impacts if they change data or try to use them for purposes other than those established by the company.
- **Recognize that new flows of information change what people consider fair.** Before the mass use of cyberspace, flows of information were limited and subject to the controls of business processes that were not up for discussion. With permanent and open access to information, people sense that much of what they have or receive should also be in the public domain. In this regard, access to information should not be a restriction, but an opportunity to know more, which, in the context of companies, generates contradictions and serious discussions on regulations and legal concepts.[5]

The same thing happens with personal information. It is not the control of access that changes a person's way of thinking, but rather the use of the information to which they have access. This is where the difference arises in current practices for protecting information—think of control of the use of personal information, backed up by control of access and not *vice versa*. This implies individual responsibility regarding the organization's accountability for the information of its clients, employees or involved third parties.[6]

Proposal of a Privacy Protection Framework

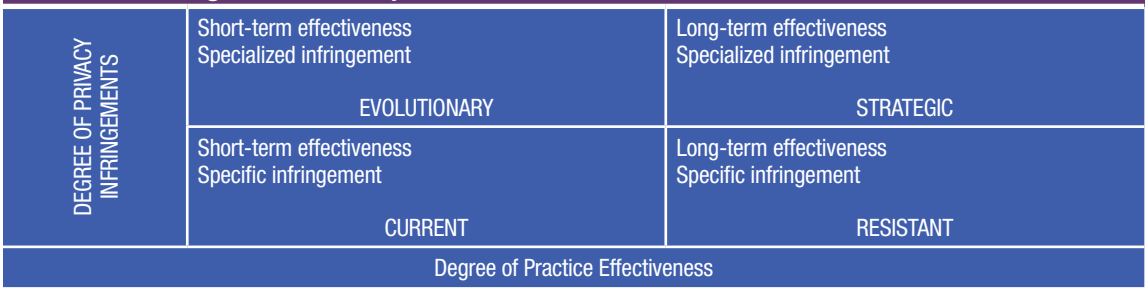
Considering the new normal and the tensions mentioned previously, the framework of action to protect privacy must be articulated in at least the degree of privacy infringement and degree of effectiveness of the practices available at the time. These two variables focus on the people and the failures that can arise during the custody of personal information, no matter what other issues generate tension.

While there may still be other criteria used to establish a framework of action for the protection of privacy, the framework should be based on the inevitability of a violation of privacy, even though the previously mentioned context is designed for the flow of information to occur intentionally or unintentionally.

The conceptual framework illustrated in **figure 1**[7] offers four quadrants that seek to match the protection of personal information scope with specific actions that develop with the exposure of flows of information and new threats to privacy. These are generally associated with new attack vectors on information security and the appearance of services or products that require or request personal information to configure or deliver the value promise they offer.

The current quadrant indicates specific privacy infringements that are widely mentioned in international regulations and the best practices of multinational standard entities and associations, which generally are associated with inadequate practices in the processing of information. These include flaws in the final availability of information, limited security and control practices on computer

Figure 1—Conceptual Framework for Personal Data Protection



Source: J. Cano. Reprinted with permission.

equipment (e.g., passwords, encryption, information backup), and extraction of falsely obtained information (social engineering).[8]

In such cases, there are security and control practices that are applicable immediately and in the short term, allowing an increase in the resistance of the organization in the case of a leak or loss of personal information. These end up being standards for the people in charge of such information and, in general, for everyone at the company who recognizes that personal information is a right of which each employee becomes the guardian.

The resistant quadrant is an area that illustrates specific infringements of privacy (mentioned in the current quadrant) in which established practices have the challenge of incorporating a permanent and formal reference for the protection of personal information in the collective imagination of the individuals of the organization. This should be a generic competency of companies that recognize the value of information and respect the rights and guarantees of citizens when processing their personal information.

To achieve this competency, it is necessary to develop activities related to awareness, internalization, appropriation and compliance with practices for the protection of information as a foundation for the appropriate and competent behavior of people with regard to privacy. Here, top management is not only ultimately responsible for the consequences of improper processing of information, but also the main interested party in the training and configuration of a scenario that recognizes privacy as a right of individuals and as a duty of compliance of the company.

The evolutionary quadrant represents the challenge that new attack vectors[9, 10] create, and it is where known practices are insufficient to facilitate the protection of personal information. Attacks such as advanced persistent threats (APTs), ransomware and malware codes (even malware in mobile systems) are examples of new realities that have effects on privacy, which compromise good practices that organizations may have in place, given the multiple and varied forms in which they can occur.

In this context, known security and control practices can have limited effectiveness, hence the need to study in detail extended strategies for the protection of information, both in its flow and source. These, even if they do not prevent privacy infringement, still establish additional actions, such as data encryption[11] and specific views of duly monitored access, Internet Protocol (IP) addresses and authorized localizations, previously registered and authorized devices and applications, double authorizations for access, and schedule control and control figures (among other activities), which make flows of information more resilient to undesired disclosures or losses of information.

The strategic quadrant is the greatest challenge for the person responsible for the protection of information in an organization. He/she must keep a current view of the privacy threats to the company, configuring extended protection practices such

as those mentioned in the evolutionary quadrant, ensuring a continuous transformation of the collective imagination regarding privacy adjusted to the demands of the environment and the supervisory bodies, as well as the expectations of clients and users.

To achieve this, an extended privacy impact analysis is required, which will not only take into account the known and reported privacy risk, but will also consult latent, emerging and industry threats and risk.[12] This is intended to motivate preventive actions regarding this scenario and to anticipate practices that will increase the company's resistance against specialized privacy infringements and will, therefore, strengthen its framework for appropriate care of personal information protection for every interest group.

Conclusion

There is no doubt that in an interconnected world with geopolitical tensions, information is of crucial importance and helps define political, economic, social and administrative strategies in a society of information and knowledge. The control and management of information for decision making establishes a natural point of reference of modern management, which understands that information has potential power for those who have it, and its final use is determined by their legitimate access and intentions.

Every time there is a digital modification of products and services for those with access, the flows of information that are generated allow greater identification of individuals. Given this environment, it becomes clear that privacy is a challenge for individuals, organizations and nations—a challenge that creates tension and builds dilemmas in which the benefits for some are disadvantages for others.

In this sense, the proposal of a conceptual framework for protection that is presented in this article seeks to reconcile the internal practices of organizations with the requirements of the environment and the inevitability of privacy infringement. The intent is to establish an intelligent effort, which, taking into account the tensions this subject generates and the new normal that we must understand for personal information protection, allows the construction of an evolutionary privacy strategy that will show the maturity of the personal information protection program in an organization. Regardless of the changes in regulations, behaviors and habits of people, and the new attack vectors on information security that constantly arise, the suggested conceptual framework on privacy must adapt in order to mature in the environment that is imposed on it. It is up to the organization, each of its employees and, in particular, the executive who is responsible for the protection of personal information to define the proposed quadrants to build an understanding of privacy adapted to the company's reality that will strengthen the scenario of respect for, commitment to and compliance with the dignity of the people and their self-determination regarding personal information.

“Every time there is a digital modification of products and services for those with access, the flows of information that are generated allow greater identification of individuals.”

Endnotes

1 Federal Trade Commission, *Internet of Things: Privacy & Security in a Connected World*, FTC Staff Report, USA, January 2015, *https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf*

2 Bodell, L.; "Five Steps to Formalizing Forward Thinking in Your Organization," *Strategy+Business Blogs*, 4 January 2016, *www.strategy-business.com/blog/Five-Steps-to-Formalizing-Forward-Thinking-in-Your-Organization*

3 Cano, J.; "Privacidad en las conversaciones electrónicas. Cuatro perfiles para analizar," IT-Insecurity blog, 25 October 2015, *http://insecurityit.blogspot.com.co/2015/10/la-privacidad-en-las-conversaciones.html*

4 Austin, R.; D. Upton; "Leading in the Age of Super-Transparency," *Sloan Management Review*, 14 December 2015, *http://sloanreview.mit.edu/article/leading-in-the-age-of-super-transparency/*

5 *Ibid*.

6 Smith, J.; "Demanding Accountability: The Need for Cyber Liability," *Help Net Security*, 4 January 2016, *www.net-security.org/article.php?id=2436*

7 Stewart, G.; "The Security Advice Magic Quadrant," *ISSA Journal*, February 2016, http://*www.bluetoad.com/publication/index.php?i=-286807&m=1336&l=1&p=7&pre=*

8 Krausz, M.; J. Walker; *The True Cost of Information Security Breaches and Cyber Crime*, IT Governance Publishing, UK, 2013

9 Goodman, M.; *Future Crimes: Everything Is Connected, Everyone Is Vulnerable and What We Can Do About It,* Doubleday, USA, 2015

10 Zetter, K; "The Biggest Security Threats We'll Face in 2016," *Wired*, 1 January 2016, *www.wired.com/2016/01/the-biggest-security-threats-well-face-in-2016*

11 Greenberg, A.; "The Father of Online Anonymity Has a Plan to End the Crypto War," *Wired*, 6 January 2016, *www.wired.com/2016/01/david-chaum-father-of-online-anonymity-plan-to-end-the-crypto-wars/*

12 Cano, J.; *La ventana de AREM. Una herramienta estratégica y táctica para visualizar la incertidumbre. Actas de la XIII Reunión Española de Criptología y Seguridad de la Información*, RECSI 2014, Alicante, Spain, 2-5 September 2014, *http://web.ua.es/es/recsi2014/documentos/papers/la-ventana-de-arem-una-herramienta-estrategica-y-tactica-para-visualizar-la-incertidumbre.pdf*