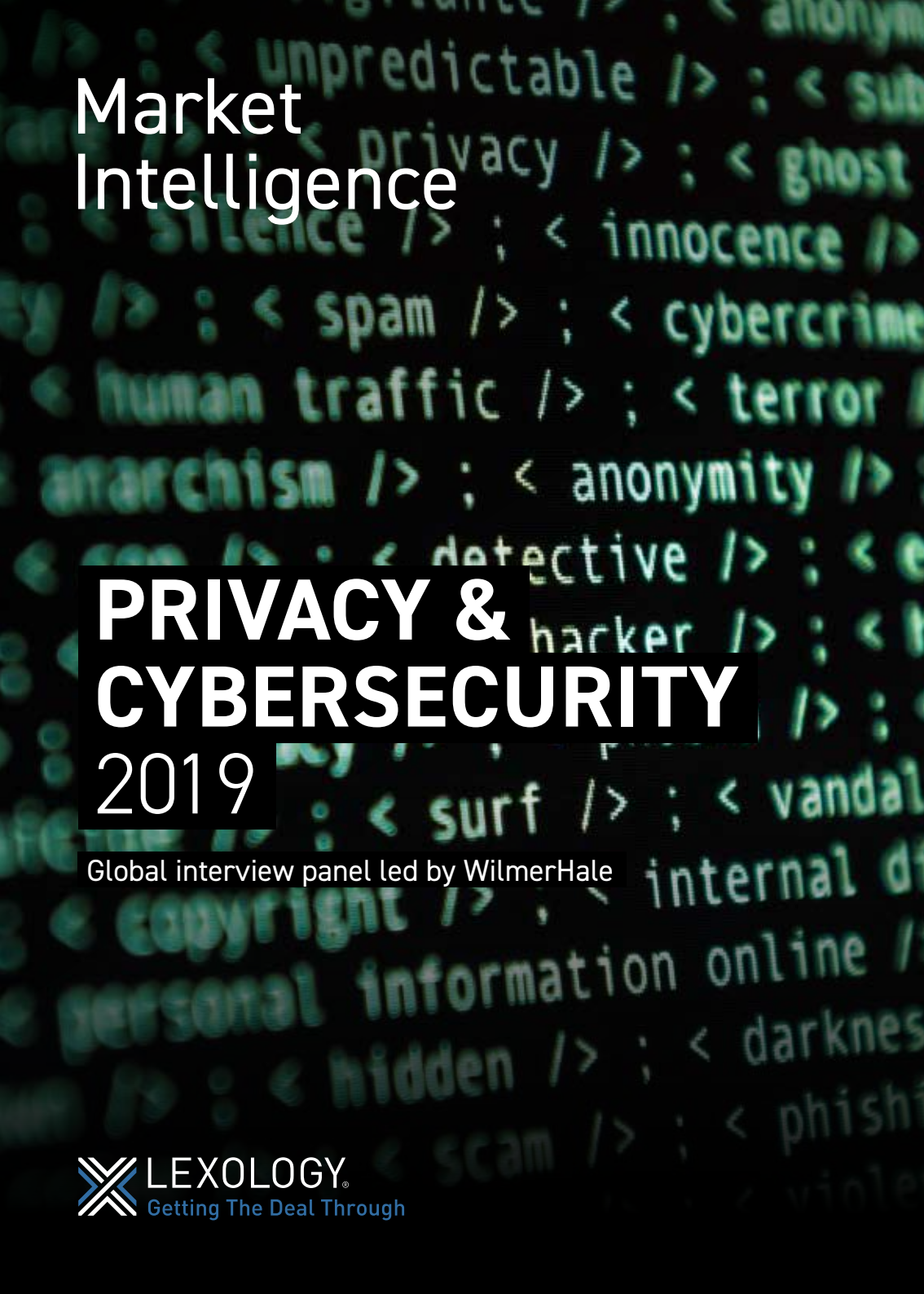
Market
Intelligence
PRIVACY &
CYBERSECURITY
2019
Global interview panel led by WilmerHale
LEXOLOGY
Getting The Deal Through

Mexico

Begoña Cancino, partner of the IP practice at Creel, García-Cuéllar, Aiza y Enríquez, SC, has taken the lead since the issuance of the Mexican Privacy Law. This approach of handling data privacy matters on the basis of an IP expert has been very successful, as personal data is assembled in databases that constitute a work of authorship under the Mexican Copyright Law and also constitute confidential information that may qualify as a trade secret under the Mexican Industrial Property Law. Begoña's IP background gives her a better sense of her clients' needs and the different angles that should be considered when providing the most specialised advice in the field.

Begoña has authored several articles for the *World Intellectual Property Review* ('Protecting Data in Mexico: what you need to know'), as well as published since 2015 and 2016 editions of *The Data Protection and Privacy Global Guide* and IP *in Business Transactions* by Thomson Reuters. She also authored the Mexican chapters for the *International Comparative Legal Guide on Data Privacy*, *Cybersecurity*, as well as *Gambling* since 2017.

Begoña received her law degree from Universidad La Salle in 2001; postgraduate studies at the University of Buenos Aires; Universidad Nacional Autónoma de Mexico and participated in the Leadership and Management Program for Lawyers, both at the Yale School of Management.

Sofía Castañón is a junior associate in the Mexico City office. She joined the firm in 2014 and graduated from Universidad Anáhuac Mexico City in 2016. She specialises in the IP, data privacy and advertising areas, mainly advising on registration, licensing, transfer and the maintenance of IP rights.

1 What were the key regulatory developments in your jurisdiction over the past year concerning cybersecurity standards?

During the past year, there have not been any material amendments to the Mexican data protection laws and its regulations (Mexican Privacy Law). However, on 12 June 2018, it was published in the Mexican Official Gazette that Mexico had adopted the Council of Europe Convention 108 of 28 January 1981 for the 'Protection of Individuals with regard to Automatic Processing of Personal Data' and its 'Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and cross border data flows'. Both are binding international instruments that protect the individual against abuses that may accompany the collection and processing of personal data and seeks to regulate, at the same time, the cross-border flow of personal data.

Additionally, the National Institute for Transparency, Access to Information and Protection of Personal Data (INAI) – the autonomous constitutional body that guarantees the protection of personal data and access to public information right in Mexico – recently issued the following resolutions on data protection matters, which were transcendental in Mexico.

Pegasus software

In 2017, the Peña Nieto Administration acquired a surveillance software called Pegasus, which was allegedly used by the Attorney General's Office (PGR) to spy on journalists, activists and human rights advocates.

Among other authorities and proceedings, the INAI conducted a software verification process. The INAI determined that the PGR did not comply with the security and responsibility duties to process and transfer personal data set forth in the Mexican Privacy Law, since the software was being used to collect personal data and generate databases for storage, without having a proper a management system and security logbook for such purposes. In addition, the PGR did not undertake the adequate procedures to carry out the safe deletion of the data after such software's uninstallation. Therefore, as a result of the verification process, the INAI instructed the PGR to prove that the Pegasus software had been uninstalled, as well as the measures taken to guarantee that is not feasible to reinstall it.

Penalty for the disclosure of personal data

Recently, the Savings and Financial Services National Bank (BANSEFI), while updating its website contents, disclosed certain personal data of its clients, including bank accounts information. The INAI instructed the internal compliance organ of BANSEFI to punish the employee responsible for disclosing such information.


Begoña Cancino


Sofía Castañón Rivera

2 When do data breaches require notice to regulators or consumers, and what are the key factors that organisations must assess when deciding whether to notify regulators or consumers?

The Mexican Privacy Law regulations provide that the data controller must inform only the data subject, not the federal regulator or other authority. As per the timeline, the regulations only provide that such notifications should be conducted without delay and, of course, after assessing if the breach significantly affects the property or non-pecuniary rights of the data subjects upon having conducted an exhaustive review of the magnitude of the breach so that the prejudiced data subjects may take the appropriate measures.

3 What are the biggest issues that companies must address from a privacy perspective when they suffer a data security incident?

Companies shall confirm first if personal data is compromised and if so, what type of personal data was (sensitive or not) and how many subjects were affected by the

breach (this, along with the proper identification of the affected parties, which is crucial for notification purposes). In addition, companies must have to implement corrective, preventive and improvement steps to make the security measures adequate to avoid a repeated breach. These measures should be informed to the data subjects, along with the nature of the breach, the personal data compromised, the recommendations to data subjects after the breach and the means available for data subjects to obtain more information of the event, if that notification is necessary, under Mexican provisions.

4 What best practices are organisations within your jurisdiction following to improve cybersecurity preparedness?

To be prepared for a security incident and improve security measures within the company, the Mexican regulations provide that companies comply with certain obligations as data controllers, such as:

- prepare an inventory of personal data and processing systems;
- determine the duties and obligations of those who process personal data;
- make a risk assessment, establish security measures and identify those effectively implemented so far;
- analyse the gap between existing security measures and those missing but necessary for the protection of personal data;
- prepare and update a work plan for the implementation of the missing security measures arising from the gap analysis; and
- train personnel and keep a record of personal data storage media.

5 Are there special data security and privacy concerns that businesses should consider when thinking about moving data to a cloud hosting environment?

The Mexican Privacy Law provides that any (national or international) transfer of personal data to third parties (other than data processors) generally needs to be set forth in the privacy notice and requires the consent (express or implied, as the case may be) of the relevant data subject. Cloud hosting companies might process personal data under data controller's instructions and on its behalf and therefore might be considered as data processors. Although the transfer of personal data to data processors does not need to be disclosed in the privacy notice, nor does it require the consent of the relevant data subjects, companies will be required to communicate the corresponding privacy notices to any such third parties and adopt necessary measures to ensure that they comply with the terms of such notices and

"Cloud hosting companies might process personal data under data controller's instructions and on its behalf and therefore might be considered as data processors."

the Mexican Privacy Law, which might accomplished through the execution of a written agreement with such data processors.

In addition, considering that cloud computing is a model for the external provision of computer services on demand that involves the supply of infrastructure, a platform or software distributed in a flexible manner, using virtual procedures, on resources dynamically shared, a data controller should enter into service agreements with at least the following contractual conditions for the service provider:

- it shall use similar policies to protect personal data as those reflected in Mexican Privacy Law;
- if the service provided involves subcontracting, such provisions should be transparent;
- it should not assume any ownership on the information about which the service is provided; and
- it should maintain confidentiality with respect to the personal data about which it provides the service.

Photo: istock.com/@Elijah-Lovkoff

"The federal police have created a scientific division specialised in providing assistance to the victims or claimants of cyberthreats and cyberattacks."

6 How is the government in your jurisdiction addressing serious cybersecurity threats and criminal activity?

Public prosecutors in Mexico are in charge of investigating cyber activities and to resolve them, a cyber police force has been created to follow up on crimes or unlawful activities committed through the internet. Complaints directed to the cyber police can be submitted via its website, by phone or through a Twitter or email account; in addition, the federal police have created a scientific division called the National Centre For Cyber-Incidents Response, specialised in providing assistance to the victims or claimants of cyberthreats and cyberattacks.

In the case of data protection, the INAI may conduct investigations to follow up personal data matters. Regarding telecommunications, the Federal Telecommunications Institute is in charge of this sector. Regarding software, the Mexican Institute of Industrial Property also has investigatory powers.

7 When companies contemplate M&A deals, how should they factor risks arising from privacy and data security issues into their decisions?

In M&A deals companies must be cautious from the very beginning about the pitfalls around exchanging and processing personal data and the different treatment of such data in every stage of the process, whether the matter is a purchase of assets or a purchase of stocks. Depending on the type and purpose of the M&A process, companies should think about splitting the case into stages and using mechanisms to preserve such information in confidentiality as long as possible, by implementing anonymisation proceedings, being very focused on complying with the duty of confidentiality and, also, ensuring their own representatives execute non-disclosure agreements sufficiently astringent as the stage of the process requires. At certain point, companies will be prepared to disclose key information to the other party and that would imply the execution of a new document allowing the exchange and level of information sought to be disclosed. Companies representatives should monitor the use of all personal data provided within the context of the M&A transaction, in order to be sure that no one will be misusing the information and, by doing so, putting the company at risk. A manual of good practices when processing personal data should facilitate the communication between the parties and the analysis of personal data.

Begoña Cancino Garín
begona.cancino@creel.mx

Sofía Castañón Rivera
sofia.castanon@creel.mx

Creel, García-Cuéllar, Aiza y Enríquez
Mexico City
www.creel.mx

The Inside Track

When choosing a lawyer to help with cybersecurity, what are the key attributes clients should look for?

A lawyer specialised in cybersecurity should be able to differentiate between material and non-material harm under Mexican law by conducting a risk assessment to provide client with alternatives to move forward to avoid breaches and misuse. Lawyers should also have a good relationship with the Mexican regulator.

What issues in your jurisdiction make advising on cybersecurity and privacy complex or interesting?

The fact that terms such as 'cybercrime' and 'cybersecurity' are understood as criminal actions carried out by individuals who use information and communication technologies as a means or as an end and that are typified in a criminal code or other national code.

How is the privacy landscape changing in your jurisdiction?

Mexico has adopted the Council of Europe Convention 108 of 28 January 1981 and its additional protocol (see question 1). Both are binding international instruments that protect the individual against any abuse in the collection and processing of personal data and at the same time seek to regulate the cross-border flow of personal data. On 9 September 2017, the Officer of the General Prosecutor announced a new investigation unit created to combat cyber- and technological crimes and enhance investigations. The unit is actively working with the Bank of Mexico to identify and sanction all those responsible for a cyberattack on several financial institutions.

What types of cybersecurity incidents should companies be particularly aware of in your jurisdiction?

The most common enforcement actions taken by authorities are related to the breach of systems with the purpose to obtain personal data (either sensitive or financial data) for profit. The private sector has been cooperative when the breach is caused by hackers, however, there are cases in which the authorities have imposed fines on the private sector, as a consequence of the breaches occurred for not having the proper security measures in place.

Lexology GTDT Market Intelligence provides a unique perspective on evolving legal and regulatory landscapes.

Led by WilmerHale, this *Privacy & Cybersecurity* volume features discussion and analysis of emerging trends and hot topics within key jurisdictions worldwide.

Market Intelligence offers readers a highly accessible take on the crucial issues of the day and an opportunity to discover more about the people behind the most significant cases and deals.

Regulatory developments
M&A risks
Best practice
Cloud hosting

ISBN 978-1-83862-199-5