

Source: Privacy & Security Law Report: News Archive > 2016 > 01/11/2016 > Special Report > Social Media: Social Media Privacy Concerns Rising in Latin America

15 PVLR 86

Social Media

Social Media Privacy Concerns Rising in Latin America

By Ivan Castano

Jan. 5 — Latin America needs stronger laws to protect workers' social media and privacy rights at a time when rising Internet penetration is raising the specter for increased litigation, according to privacy lawyers interviewed by Bloomberg BNA.

Very few nations—notably Colombia and Argentina—have worker privacy laws or judge-made privacy protections, but these remain weak and ambiguous, they said. Mexico has yet to address the issue, but its data protection agency has a bill in the works for this spring (14 PVLR 2329, 12/21/15).

Against this backdrop of legal uncertainty, employer-written social media and privacy policies can shape employee expectations and minimize the risk of hefty employer fines by data protection authorities, these attorneys told Bloomberg BNA.

"We need a deeper technology work culture and companies willing to demand clear and specific regulations for online and offline worker privacy to spur such legislation," Guillermo Zamora, of Zamora & Associates in Trelew, Argentina, told Bloomberg BNA. "The issue needs to be taken seriously and at the legislative level."

Only Colombia Has Social Media Law

Colombia is the only Latin American nation with a specific law protecting privacy interests in social media accounts. Enacted in 2009, Ley 1273 authorizes courts to impose monetary penalties on employers that monitor employees' social media or other Internet activities without their consent (8 PVLR 43, 1/12/09).

"No one can go into anyone's personal profile without obtaining authorization," Alvaro Soto of Asoto Technology Group in Bogota, Colombia, a company that does forensic work in privacy lawsuits, told Bloomberg BNA. "Colombia has the region's most advanced legislation on this issue."

Violations of Ley 1273 can be punished with up to 96 months in jail and up to \$300,000 in fines. Colombia also recently increased penalties for violations of the country's data protection framework.

"Companies are starting to meet Ley 1273 from fear of facing fines," Soto said. Very few Colombia-based employers comply with Ley 1273's requirements, according to Soto, though he expects that number to rise sharply.

"This is going to become a war zone," Soto said. "Companies are going to start seeking more protection and employees more privacy."

Brazil Suits Prompt Protections

Laine Souza, an IT privacy lawyer in Uberlandia, Brazil, told Bloomberg BNA that Brazil, Latin America's second-largest economy, doesn't regulate social media at work.

"The law doesn't say 'You can or cannot' monitor workers' use of social media or the Internet," Souza said.

However, judicial decisions have established jurisprudence that makes it advisable for employers to annually inform employees that their social media interactions or online browsing can be monitored.

"The labor court has ruled companies can monitor workers during their work time if they say this in their internal policies," Souza said.

Many companies were slow to introduce such policies, triggering over 100 lawsuits now awaiting court resolution, according to Souza. She expects their number will rise as Brazilians become increasingly aware of their online privacy rights.

Social Media Popular in Latin America

Brazil has the largest number of Internet users in Latin America with 112.7 million, accounting for 34 percent of 331.7 million users, according to eMarketer. By 2018, all of Latin America is expected to have 378.3 million Internet users.

Roughly 90 percent of Brazilian multinational corporations have introduced in-house policies to regulate social media usage though most small and mid-sized firms still lack them, Souza said.

In Brazil, having a social media policy is a good idea, Souza said, because the country's left-leaning labor tribunals tend to see Facebook and Twitter as good tools to relieve worker stress.



"The courts love social media," Souza said. "They don't have a problem with workers using it for a reasonable time during their shift, like 30 minutes in the morning or 30 minutes in the afternoon, or even during breaks. This fact has been established in past rulings."

Brazil is also unlikely to pursue

legislation in the foreseeable future because it doesn't want to pressure companies writhing under a stinging recession, according to Zamora.

"I don't see this becoming a legislative priority in Latin America in the short to medium term," he said, adding firms will continue to regulate the issue on their own.

Zamora expects firms will more quickly introduce in-house policies to avoid future worker lawsuits amid a booming digital culture and citizens' rising awareness of their privacy rights.

Argentinian Court Creates Privacy

Argentina has no law specifically directed to social media privacy, but there have been court rulings creating privacy rights for employees.

Argentinian courts have ruled that employees have a right to forbid their employers from monitoring their social media activities, e-mail messages and other Internet use, according to Zamora.

"If you are going to monitor, judges have said you must tell employees and you must do so periodically," Zamora said. "There is an expectation that online accounts are private."

Court rulings notwithstanding, Zamora said, most employers track their workers' social media and Web clicks without notifying them because local data protection authorities have yet to impose penalties for violations of online privacy rights.

Compliance with the law is highest among technology companies, Zamora said, adding that most small and mid-sized firms don't follow the law at all.

Mexico Lags, Costa Rica Advances

Mexico is the region's biggest laggard with social media seen as "a neglected area of government regulation," Internet privacy lawyer Joel Gomez, of the Ibero-American Observatory of ICT Policy and Legislation in Mexico City, told Bloomberg BNA

However, given the issue's rising importance in the U.S., Mexico's top trading partner, attorneys expect Mexican multinational corporations will begin tackling social media and online privacy in future internal regulations and employee contracts.

More than 50 percent of companies use device-management software to monitor their employees' social media and other online activities on or off work, according to Gomez.

"This has to be regulated, either by modifying the federal labor law or the federal data protection law in possession of private parties," he said.

Mexico's data-protection watchdog, the National Institute for Transparency, Access to Information and Protection of Personal Data (INAI), expects to tackle the issue in a new Federal Data Protection Bill slated for the spring.

The data-protection watchdog hopes to introduce rules banning "excessive monitoring" of employees during or outside work, INAI official Edgardo Martinez told Bloomberg BNA. He added such provisions will likely mirror European legislation granting employees more rights than employers, by contrast to U.S. policy.

To contact the reporter on this story: Ivan Castano in Mexico City at correspondents@bna.com

To contact the editor responsible for this story: Thomas O'Toole at totoole@bna.com

Source: Privacy & Security Law Report: News Archive > 2015 > 12/14/2015 > International News > Employment Issues: Attorneys Say Mexico Ripe for Social Media Privacy

14 PVLR 2280

Employment Issues

Attorneys Say Mexico Ripe for Social Media Privacy

By Ivan Castano

Dec. 7 — Legislation is needed to prohibit Mexican employers from engaging in widespread monitoring of employees' social media, e-mail messages and other online interactions, attorneys told Bloomberg BNA Dec. 7.

"Social media is one of the last areas of government regulation," Joel Gomez, a Mexico City-based lawyer specializing in Internet privacy, said. "This has been a big issue in the U.S. lately, but here it's not even being proposed. I don't understand why. There is null privacy at work."

Corporate attorneys in Mexico, following U.S. developments, are advising firms to modify their internal regulations or employment contracts to notify workers that workplace computers and mobile devices may be monitored.

Gomez told Bloomberg BNA that over 50 percent of large Mexican companies use device management software to monitor employees' behavior at or off work, including their social media, e-mail and Web-browsing activities, leaving them without an option to opt-out of such surveillance.

Juan Mijares, president of the International Chamber of Commerce Mexico's Digital Economy Commission, told Bloomberg BNA that large Internet firms like Google Inc., Apple Inc. and Microsoft Corp. have started informing workers they can monitor their Facebook, Twitter or other social media activities.

These firms fail to inform their workers that they will also monitor personal e-mails and anything inside an employer-owned computer, including its data cache—which employers can use as "character destruction" evidence in potential employment lawsuits, he said.

Most Businesses Monitor Workers

Over 80 percent of large Mexican businesses monitor workers, Mijares said, adding that their efforts often lack sophistication because many companies don't have a large information technology team.

Some heavyweight multinationals like telephone giant Telmex, brewer Modelo or industrial conglomerate Grupo Mexico, engage in more sophisticated monitoring.

"Some companies go a little far and are even obsessed," Mijares said. "They want to know where loyalties stand, both for current and former workers. The time has come for work privacy legislation in Mexico."

Mijares said Mexico's data protection agency, the Instituto Nacional de Transparencia (INAI), should take on the job of drafting such provisions, possibly by modifying the country's framework data protection statute or creating a new law.

The DPA should follow European legislation, he said, "because it's better developed in protecting individuals than U.S. law" and would likely face less opposition from Mexico's labor unions, which are known for blocking anything that can negatively impact workers' rights.

To contact the reporter on this story: Ivan Castano in Mexico City at correspondents@bna.com

To contact the editor responsible for this story: Alexis Kramer at akramer@bna.com

Source: Privacy & Security Law Report: News Archive > 2015 > 08/24/2015 > Special Report > Enforcement: Mexico Privacy Enforcement on Upswing in 2015

14 PVLR 1559

Enforcement

Mexico Privacy Enforcement on Upswing in 2015

By Ivan Castano

Aug. 18 — Mexico's data protection authority—the National Institute for Transparency, Information Access and Data Protection (INAI)—intends to levy total fines for 2015 of 50 million pesos (\$3 million), up from 45 million pesos (\$2.7 million) in 2014, INAI Data Protection Coordinator Gustavo Parra told Bloomberg BNA.

Most penalties will be assessed in the insurance, mass-media and financial sectors, he said, adding that debt collectors are under greater scrutiny by the regulator amid a slew of consumer complaints that they are selling data to third-party marketers.

The INAI is also looking at suggesting in mid-2016 changes to the country's framework privacy statute, the Federal Law on the Protection of Personal Data Possessed by Private Parties, Parra said. For example, the law should be modified to more strongly specify that the INAI has jurisdiction over social media companies operating in the country, regardless of where they are headquartered, he said.

The framework law "is no longer relevant " and must be updated, INAI Commissioner Oscar Guerra said in a recent statement.

INAI President Ximena Puente told Bloomberg BNA that the data protection authority, which was restructured in May and rechristened as the INAI after previously being known as the Federal Institute for Information Access and Data Protection (IFAI), has ongoing enforcement efforts regarding Google Inc., AT&T Services Inc. and department store chain El Puerto de Liverpool S.A.B. de C.V.L.

Right to Forget Decision

In January, the privacy regulator ordered Google to comply with a data subject's request to remove search engine links and threatened sanctions (14 PVLR 259, 2/9/15), Puente said. A fine of 44 million pesos (approximately \$2.7 million) has been suspended while Google's appeal in this first right to be forgotten case is considered in court, he said.

The case pits Mexican businessman Carlos Sánchez de la Peña, who owns the Grupo Estrella Blanca bus company, against the Internet search giant. Peña asked Google to delete links revealing his friendship and business alliances with former Mexican President Vicente Fox and his family, but Google refused, prompting the INAI's intervention.

Joel Gomez, an attorney with Lex Informatica Abogados in Mexico City, told Bloomberg BNA that the ANNA needs to take a chapter from European data protection regulators who moved aggressively to establish their jurisdiction to enforce right to be forgotten issues under European Union jurisprudence.

Google and Facebook Inc. are flouting the Mexican data protection statute, Gomez said. Companies argue that, because their headquarters are in the U.S. and not in Mexico where they only have marketing and administrative offices, they shouldn't be subject to Mexican law, he said. The companies also cite user terms of service that specify that conflicts must be handled in the U.S., he said.

Cedric Laurant, an attorney with Dumont, Bergman, Bider & Co. in Mexico City, said the INAI's handling of the Google right to be forgotten case was "very weak and badly made." The ANNA must strive to establish its authority against online companies with stronger decisions that reinforce its jurisdiction over them.

"These companies are selling Mexicans' data to advertisers. They are using it for any purpose. They have to comply with the law."

Cedric Laurant, Dumont,

"These companies are selling Mexicans' data to advertisers," Laurant said. "They are using it for any purpose. They have to comply with the law."

AT&T Call Center Breach

Meanwhile, AT&T's Mexican subsidiary

Bergman, Bider & Co., Mexico City

Teleperformance is also under investigation after an April data breach may have risked the records of nearly 69,000 AT&T U.S. customers, Puente said.

In April, the U.S. Federal Communications Commission announced that it had reached an administrative consent order with AT&T that included a record \$25 million settlement payment to resolve an investigation into data breaches involving almost 280,000 U.S. mobile device customer accounts operated by the company's international call center contractors in Mexico, Colombia and the Philippines (14 PVL 633, 4/13/15).

The INAI must sharpen its teeth against the companies it is investigating, as well as Uber, which the INAI hasn't investigated despite complaints it is violating customer privacy rights, Gomez said.

Department Store Hack

The INAI recently stepped up a January probe against retailer Liverpool for failing to inform customers its databases were hacked in December 2014, potentially exposing information on as many as 3.5 million credit card customers. Personal information about the company's top executives was also breached.

Liverpool has been opaque about the matter, saying only that the attack stemmed from a "bribery attempt" to "ruin its reputation," though it did notify the regulators of the Mexican stock exchange (BMV), Puente said.

Privacy attorneys have alleged that the 100-store retailer broke the law by failing to immediately inform customers about the breach, though it did notify some large account holders.

Soon after the breach, Mexican hacking group SickKillers claimed responsibility, posting photos of Liverpool's senior managers on tech website FayerWayer.com and asking, "if they can't take care of their private documents, do you think they can take care of yours ...?"

The organization claimed it has had full access to Liverpool's systems for six years.

INAI Audits Director Jonathan Mendoza told Bloomberg BNA that the INAI entered the verification phase of its investigation June 15. Liverpool has 180 days to respond to the INAI's information requests and cooperate with the probe, he said.

The INAI hopes to conclude its probe in October and may issue a fine, Mendoza said.

Gomez said Liverpool has reinforced its information technology systems since the hack. He said 70 percent of Mexican retailers remain vulnerable to data hacks and that most of them lack privacy officers.

Some, however, are taking action, swapping external security companies for internal officers and introducing better software, Gomez said.

Previous Enforcement Effective?

The INAI and its predecessor IFAI have imposed 141.7 million pesos (\$8.7 million) in data breach fines since 2012 when the country's framework privacy statute, the Federal Law on the Protection of Personal Data Possessed by Private Parties, took effect.

In its biggest fine in 2015, the INAI recently told Bloomberg BNA that it has slapped a \$2 million fine on Mexico's third-largest bank, Grupo Financiero Banorte, for allegedly failing to notify customers about a data breach in late 2014 or early 2015 (14 PVL 1531, 8/17/15).

Parra said that over the last couple of years the INAI fined Mexican mobile phone operator Radiomovil Dipsa SA (Telcel) 26 million pesos (\$1.6 million), Mexican bank Banamex 27 million pesos (\$1.64 million) (12 PVL 1038, 6/17/13), the Universidad Intercontinental school 10 million pesos (\$609,765) and BBVA Bancomer 6.6 million pesos (\$402,430).

Although welcoming the INAI's efforts to tackle the nation's privacy woes, Gomez said the regulator must do much more. Crucially, it must increase transparency by telling citizens which companies have appealed its sanctions and which have won or lost. This is crucial to gauge if the INAI is being efficient, he said, and will discourage losing companies from engaging in future violations.

"It's possible to pursue nullity trials with the Federal Tribunal for Fiscal and Administrative Justice," Gomez said. "In fact, most companies have appealed and my feeling is many have won," he said.

"It's very convenient for INAI to brag about fining companies but not who's winning," Gomez said, adding that the INAI has yet to collect most of the assessed financial penalties.

Continuing Education

Puente said the INAI will make educating companies on their compliance obligations a priority and will inform citizens about those rights amid a weak privacy culture in Mexico.

"Only 74 percent of companies understand the importance of personal data and just 45 percent have issued privacy notices," she said. The financial and educational sectors have the strongest data security measures in place, she said.

The regulator will also speed up efforts to encourage companies to pursue self-regulatory privacy and security schemes, Puente said. Uptake of the schemes has been slow as only 40 percent of companies have so far adopted them, she said.

The INAI launched a certification system Aug. 1 to help companies implement self-regulatory programs. Adopting a program will improve a company's relationship with data subjects and the regulator and help avert possible fines, the INAI said in a statement.

The system will employ third-party certification companies to "constantly audit, review and surveil" a company's data protection management, the INAI said, adding that the Economy Ministry will help oversee it.

The INAI has posted a privacy notice generator on its website and is entering data protection partnerships with business and consumer organizations, the latest of which involves Mexico City's Chamber of Commerce and the Mexican Academy of Information Technology Law, the INAI said.

To contact the reporter on this story: Ivan Castano in Mexico City at correspondents@bna.com

To contact the editor responsible for this story: Donald G. Aplin at daplin@bna.com

Source: Privacy & Security Law Report: News Archive > 2014 > 03/31/2014 > International News > Enforcement: Mexican Companies Vulnerable to Hacking As Data Security Rules Compliance Lags

13 PVLR 566

Enforcement

Mexican Companies Vulnerable to Hacking As Data Security Rules Compliance Lags

By Ivan Castano

March 20 — Mexican corporations are “very vulnerable” to hacker attacks similar to those that recently hit U.S. retailers because they have extremely low data security standard compliance rates, Juan Mijares, director of the International Chamber of Commerce-Mexico Digital Economy Commission, told Bloomberg BNA March 20.

Mexican retailers, save for large department store chain operators, such as El Palacio de Hierro or El Puerto de Liverpool S.A.B. de C.V., aren't in compliance with data security rules and are increasingly vulnerable, Mijares said.

They could fall prey to payment card hacking, such as the incidents that hit Target Corp. (12 PVLR 2133, 12/23/13) and Neiman Marcus Group Ltd. (13 PVLR 370, 3/3/14) in the U.S., he said.

Malware Attacks on Rise

Malware attacks are also increasing in Mexico, Mijares said.

Although the organized criminal groups active in the U.S. haven't reached Mexico, it “is only a matter of time” before they do, making it even more important that businesses comply with the data security provisions of the country's data protection framework statute, he said.

Only 15-20 percent of companies meet the data security standards, Mijares said.

Government databases are also vulnerable to attack, he said.

Data breach notification by corporations and the government should be mandated, he said.

Effective Enforcement?

Mexico's framework data protection law was enacted in July 2010 (9 PVLR 1016, 7/12/10), and its implementing regulations were finalized in December 2012 (11 PVLR 41, 1/2/12).

The deadline for companies to implement the security provisions of the law was June 21, 2013.

However, the data protection authority—the Federal Institute of Access to Information and Data Protection (IFAI)—didn't release data security guidelines for covered entities until October 2013 (12 PVLR 1951, 11/18/13).

The law authorizes fines of up to \$3 million, but the IFAI has been criticized for not being more active in assessing penalties for lax data security (12 PVLR 1171, 7/1/13). The largest fine assessed by the IFAI to date, a \$1.3 million fine levied against Banamex, which describes itself as Mexico's second-largest bank, is under review on appeal (12 PVLR 1038, 6/17/13).

The IFAI's future as the primary DPA is under review by the Mexican Congress (12 PVLR 2054, 12/9/13).

Once its role is sorted out, perhaps as early as by summer, it may begin stronger data security enforcement efforts, Joel Gomez, a Mexico City-based privacy lawyer, told Bloomberg BNA March 19.

Companies should begin working toward compliance in anticipation of the possible increase in enforcement, Gomez said. He noted that it is important that companies implement data security requirements with third-party suppliers that may handle personal data.

Many companies view data protection as an unnecessary expense, Mijares said. They “are conscious of the new obligations, but they don't have any incentive to comply. They see data security as a luxury expense, but once IFAI begins to audit them and impose sanctions, I think compliance will be much stronger,” he said.

Small, Mid-Size Businesses Hurdles

Gomez said that is unlikely the IFAI's data security guidelines will become legal requirements. Many businesses, particularly small and mid-size firms, cannot afford to set up the data security systems, let alone hire a privacy manager, he said.

Mijares agreed, adding that establishing a data security management system and required staff can cost \$10,000-\$40,000.

Gomez said the IFAI could launch a set of specific data security guidelines to enable smaller businesses to comply with the law, or give them more time to comply before enforcing the law. But that move could open a "Pandora's box" of problems because the framework statute treats large and small companies alike, he said, and larger companies would complain they aren't being treated fairly.

It may be one to two more years before data security compliance significantly increases because the future of the IFAI's role as the primary DPA is itself under review, Gomez said.

Posting Privacy Notices Not Enough

Gomez said many companies have issued notices of privacy policies as required by the framework law. The problem is that they think that's enough to adequately comply with the law, he said.

"Companies must understand that issuing privacy notices means they are meeting just 30 percent of the law," he said. The "IFAI must do a better job at communicating that privacy notices are just but one requirement."

To contact the reporter on this story: Ivan Castano in Mexico City at correspondents@bna.com

To contact the editor responsible for this story: Donald G. Aplin at daplin@bna.com

Contact us at <http://www.bna.com/contact-us> or call 1-800-372-1033

ISSN 2324-6316

Copyright © 2017, The Bureau of National Affairs, Inc. Reproduction or redistribution, in whole or in part, and in any form, without express written permission, is prohibited except as permitted by the BNA Copyright Policy.