GLOBAL INFORMATION SOCIETY WATCH 2014

Communications surveillance in the digital age

This report was originally published as part of a larger compilation, which can be downloaded from GISWatch.org

Association for Progressive Communications (APC)
and Humanist Institute for Cooperation with Developing Countries (Hivos)

ISBN: 978-92-95102-16-3

APC-201408-CIPP-R-EN-DIGITAL-207

CHILE

Monitoring back

ONG Derechos Digitales
Juan Carlos Lara
www.derechosdigitales.org

Introduction

Despite being a small country, Chile has shown strong signs of being a friendly country for commerce and entrepreneurship, especially when it comes to foreign investment. This was a major trend that started under the military dictatorship, increasing over the last 25 years. A national commitment to peace, internally and externally, has allowed Chile to stand as a beacon of free trade, social peace, and steady economic growth.

In this environment, it is understandable that from a policy-making perspective, emphasis is given to the best possible conditions for entrepreneurs to carry out their business. This has included privatisation and low taxes, as well as lowering other barriers to commerce. Many say an ambience of social peace allows for better economic security. The low barriers to commerce and sense of security, along with the free market environment, extend to what has been considered one of the most important commodities of the economy of the 21st century: personal information.

While the world debates the nature of and need for the collection of personal data by governments, Chile still does not consider data privacy a matter of great concern. Unfortunately, this has led to an environment where commerce is king, even when it comes to handling the personal data of Chilean citizens. Are they safe from the processing of data by national and even foreign companies? Are Chileans safe from private surveillance, and how do international principles apply when it is businesses, not governments, that are behind the processing of data?

Background

Chile has been singled out as one of the countries with the most progressive laws regarding the internet. This includes a net neutrality law, and a copyright law that allows for notice and takedown of infringing content only when there is a court order. Several administrations have also attempted to create a "digital agenda" to promote the use of technology, and in doing so foster economic growth.

From a social standpoint, Chile stands out for being a peaceful nation in comparative terms, both in its relationship to its neighbours, as well as within the country. No important terrorist network, whether national, foreign or international, has been reported to carry out activities within the Chilean borders. Intelligence activity is focused on the possibility of social unrest and, especially, on drug cartels operating within the country.

On the other hand, the Chilean government has not been especially concerned with data privacy. Chile stands out from all other Latin American countries (except for El Salvador) because of its lack of constitutional protection of personal data, and a lack of proper legal channels for addressing different violations of data protection laws. And while practices in relation to the protection of personal information are seemingly changing in state agencies (as around the world), there have been instances of the violation of privacy rights, but without these having much impact on policy or law.

Privacy and data: When businesses have more power than states

As with any other regulatory framework that attempts to represent different interests, Chilean data protection laws occur in an environment where the interests of information privacy are not only unclear, but also unbalanced. This is not because of anything the state has done (at least, not in an alarming way). Chile has enacted some of the most progressive legislation addressing difficult issues related to technology, as the copyright reform[1] and net neutrality[2] laws have shown. Pioneering attitudes from Chilean legislators were already seen regarding data privacy: in 1999, Chile became the first Latin American country with a comprehensive data protection law.[3] However, the existence of such a law is not necessarily synonymous with a complete system of safeguards for either personal data or even privacy in general, for different reasons.

1 Law No. 20.435, 4 May 2010.
2 Law No. 20.453, 26 August 2010.
3 Law No. 19.628, 28 August 1999.

First, the national data protection law is not strictly in line with constitutional guarantees as provided by the 1980 constitution, drafted during the military dictatorship that put in place Chile's very liberal economic system. The constitution recognises several fundamental rights, including the protection of private life and the protection of private communications, but not the protection of personal data (unlike almost every other country in the region). These rights are enforceable not only against breaches by the state, but also against attacks or threats by private entities. And because personal data is not part of the constitutional framework, constitutional action can be carried out against breaches of private life or private communications, yet not against the gathering and processing of personal data. Because of this, reliance for protection must be placed upon the law directly.

Second, Chile's data protection law provides the framework for all processing and treatment of personal data, whether by public or private entities, while also respecting the rights recognised in the constitution. From a state intelligence perspective, most efforts have been linked to the collection and processing of all kinds of information with clear focuses: the so-called war on drugs, the prevention of attacks by (very minor) anarchist groups; the assessment of public perceptions regarding diplomatic or political events; and the control of indigenous communities in the southern region of the country.[4] However, the last issue is quite sensitive to changes in executive power: the current local authority empathises with much of the local indigenous community,[5] while the former authority condemned their most violent actions as terrorist (with the disagreement of the judiciary).[6]

Third, Chile's privacy rules, covering personal life, private communications and personal data, have all seemingly placed both the interests of free trade and the interests of security above other interests. This is most evident in three aspects, which we will look at in greater depth below later, that serve as examples of a national attitude towards privacy: one, by broadly allowing practices of private surveillance, for alleged security purposes, in places such as the workplace; two, by legally allowing copyright holders to send alleged online copyright infringers private notices using IP addresses; and three – and most problematically – by legally allowing any person or company to collect and process personal information, as long as they abide by the legal framework established by the data protection law. To this, we might add the legal permission to send unsolicited commercial offers (including spam email).

No control over personal data (except for companies)

Chile's data protection law allows the handling of personal data by any person or company, public or private, including the creation and transfer of databases containing personal data. This is why it is considered a set of rules for enabling the free flow of information between database traffickers. And although the law recognises a series of rights for an individual's data, these rights must be exercised through the civil courts of law, in lengthy and expensive proceedings, which constitute an insurmountable barrier for the average citizen. The lack of a data protection authority adds a lack of institutional strength to an already ineffective piece of legisation. In fact, to date, after the law has been in force for more than 14 years, following this route has resulted in no sentences for the unlawful handling of personal data. Paradoxically, it has also meant that Chilean companies are not eligible to offer certain kinds of services that require intensive handling of personal data, since the country cannot guarantee an adequate level of protection of personal data as required by the European Union.

This state of affairs has allowed personal information to circulate freely in Chile, and legally, through multiple companies dedicated to the handling of personal data. This data is frequently exchanged among companies that offer commercial, financial, health and telecommunications services, among others, seriously affecting the right to a private life guaranteed by the constitution. The existence of a unique ID number for each citizen has only made it easier to identify a set of data belonging to an individual, in practice replacing a person's name as an identifier in several information systems.

In short: Chile's privacy and personal data protection rules place those interests under the control

4 An elderly couple died in a fire in their countryside house, allegedly started by members of a Mapuche indigenous community. This led to criticism of the National Intelligence Agency due to a lack of information provided prior to the attack. Pinochet, J. (2013, November 9). La inteligencia en Chile en los tiempos de Snowden. *La Tercera*. diario.latercera.com/2013/11/09/01/contenido/reportajes/25-150344-9-la-inteligencia-en-chile-en-los-tiempos-de-snowden.shtml

5 Chile's latest change in government brought a new authority to the region, Francisco Huenchumilla, who is of Mapuche origin and who, unlike his predecessors, has called for a peaceful solution to the unrest, and an end to the classification of Mapuche activists as "terrorists".

6 Although prosecution of violent acts in Araucanía has been pursued under the Anti-Terrorism Law, the courts have systematically rejected this classification.

of private companies. Examples of this are many. Large amounts of personal data leaked from public services[7] or mishandled by banks and other private companies[8] could be subject to commercial traffic among private companies, and these practices have not been subject to legal penalties.

In 2009, a lawyer publicly accused her medical insurance company of handing over her medical information, including her medical history and diagnosis, to a chain of pharmacies. She discovered the following when purchasing medication in one of their stores: the pharmacy not only had her name and profile, but also knew her medical condition, supposedly protected not only by data protection laws, but by laws guaranteeing medical privacy. The system allowed the pharmacist to suggest medical products for this person. However, while the administrative authority fined two insurance companies, these companies claimed that exchanging this information was not only legal but also widespread, customary, and even necessary.[9] In April 2013, years after this scandal, a different insurance company proudly announced a new agreement with similar goals with a different pharmaceutical chain.[10] The 13 International Principles on the Application of Human Rights to Communications Surveillance[11] have been drafted and signed by hundreds of institutions and individuals from all corners of the world, demanding state action under strict rules of necessity, proportionality, transparency, accountability, legality and more. But it is hard to assess the damage that can be caused when, in fact, there are private companies with more information at their disposal than even the state has or could have, for the mere fact that commerce is an interest whose strength far surpasses the interests of national security.

Conclusions

Over the last several months, a great deal of public attention has been focused on the capacities of states to gather and process personal information and to conduct communications surveillance, which some have justified in the aftermath of terrorist attacks that have replaced Cold War fears in the public conscience. Such overreach of intelligence services, however, does not seem as easily justified by states which do not face the threat of war, or have more peaceful international relations. But in either case, personal information is still an important resource for different objectives.

Chile has a personal data law which from the beginning seemed to be tailor-made for big companies, and which calls into question the ability of Chile's legislators to address the problems that the information age raises for the protection of fundamental rights and freedoms. In practice, this means that personal data in Chile is not as much under the control of the state as it is in "no man's land", due to a weak set of rights and paltry enforcement mechanisms. This situation forces those who are affected to go to court to gain any effective penalties for abuses. These abuses, because they happen under the opaque practices of private companies, are beyond public scrutiny.

Several reforms to the law are currently being discussed, while some others have resulted in minor adjustments. So far, no reform bill includes the creation of an agency for the protection of personal data, which would give citizens effective tools to protect themselves from the constant abuses that exist today; nor does any bill address the free-for-all in personal information databases that is currently part of the system. Numerous groups with corporate interests seek to maintain the status quo, on the grounds that they are defending the free flow of information, and are against all obstacles that a more effective system would create for entrepreneurship.

How do principles of state surveillance apply when it is not the action of the state that endangers or threatens the interests of privacy? Unfortunately, they do not impact directly as well as they do indirectly, by reaffirming the need for privacy safeguards in any environment where the right to privacy is endangered (or any other fundamental right, for that matter). Because companies are, in this area, even more powerful than the state in their ability to affect or impact on the population, actions aimed at the state, while always convenient to ensure fundamental rights and freedoms, seem less urgent than to demand a constitutional and legal framework that ensures such freedoms are also not subject to the whims of private companies.

7 Cooperativa.cl. (2014, March 27). Investigan copia irregular de la base de datos del Registro Civil. *Cooperativa.cl.* www.cooperativa.cl/noticias/pais/servicios-publicos/registro-civil/investigan-copia-irregular-de-la-base-de-datos-del-registro-civil/2014-03-27/093754.html

8 Álvarez, C. (2012, July 3). Banco de Chile reconoce error: envió datos personales a otros clientes por correo electrónico. *Biobiochile.cl.* www.biobiochile.cl/2012/07/03/banco-de-chile-reconoce-error-en-envio-de-datos-personales-a-traves-de-correo-electronico.shtml

9 Jara Roman, S. (2009, May 26).Isapres hacen sus descargos en polémica por intercambio de información con farmacias. *Terra.* economia.terra.cl/noticias/noticia.aspx?idNoticia=200905261057_INV_78098854

10 Diario Financiero. (2013, March 27). Isapre Cruz Blanca sella alianza con Farmacias Ahumada. *Diario Financiero*.

11 https://en.necessaryandproportionate.org/text

Action steps

The protection of fundamental rights and freedoms in this day and age demands action not only to confront powerful states, but also to confront increasingly complex and powerful private entities. This requires strong action from civil society to, in the first place, educate and empower people in the rights that they hold, in order to enforce them and make others respect them.

Secondly, and addressing both private and state power, campaigns should push for the implementation of changes to the law that recognise and enforce stronger privacy rights in different areas – not only to enact the principles that should frame state action for security purposes, but also to create rules that prevent abuse by private agents.

Thirdly, constant effort is needed to ensure that any legal provisions are fully compliant with international human rights standards and the constitutional framework of Chile. This means, monitor back: demand information from public entities through transparency mechanisms, and demand active public oversight of the action of private agents regarding personal information and private communications. Such strong action will allow citizens to keep in check the threats to privacy that are wrongly touted as legal or necessary.