INTERVENTIONS

Gisela Pérez de Acha (2015)

Informe: Hacking Team malware para la vigilancia en América Latina

Website: derechosdigitales.org, 82 pp.

Reviewed by Carlos Alba Villalever
Freie Universität Berlin

When we connect to the internet, the internet connects back to us. Every day we willingly give out our personal information and those of friends and acquaintances, on whom we constantly report to services like Facebook or LinkedIn in order to remain "connected". Data about us is continually harvested, aggregated and analyzed, not only for commercial purposes, but also for mass surveillance, policing and control. The private data we leave behind as much on the internet as in our own electronic devices – search history, e-mails, text messages, phone calls, locations, address books, calendars, documents, pictures, videos, and even records of the food we eat – tells a story about us that is made up of facts that are not necessarily true. As State sanctioned surveillance practices motivate the systematized recollection of all these data and feed a growing international market for spying tools, we are losing control over the narrative of our lives by becoming increasingly vulnerable to abusive policing justified by unwarranted scrutiny.

In this context, the information that whistleblowers and activists convey to us about surveillance practices plays an important role in holding the authorities and companies involved accountable. A good example is this report, written by Mexican lawyer and activist Gisela Pérez de Acha and issued by Derechos Digitales, a Chilean NGO present in all Latin America that focuses on advocacy issues concerning fundamental human rights in the digital sphere.

In this case, the work of Pérez de Acha avails itself of a trove of more than 400 Gigabytes of data delivered to WikiLeaks by hacker Phineas Fisher that exposes the dealings of Hacking Team, an Italian information technology company specialized in surveillance and "offensive security" products for governments around the world. Through a series of leaked internal e-mails, invoices, files and source codes from Hacking Team, her report exposes the details of negotiations between this company and thirteen countries in the Latin American region: Brazil, Chile, Colombia, Ecuador, Honduras, Mexico, Panama and Argentina, Guatemala, Paraguay, Peru, Uruguay and Venezuela. Her emphasis is on the first seven countries, as for these there is actual proof of Hacking Team's products and services having been purchased, while for the other six there is only proof of communication between parties.

Hacking Team's dealings with these governments mainly involve licensing of a piece of software called "Remote Control System" (RCS), which can infiltrate almost any electronic device from a distance and take control of most of its features. RCS can turn a device's GPS, microphone and cameras on and off to track one's movements and to listen to, watch and log their activities. It can intercept, record and alter all incoming and outgoing communications, as well as access any file stored in the device and record every single character typed into it - without its owner ever knowing it.

The report has a straightforward structure. The summary provides a brief overview of the work's problem, objectives and findings. A succinct introduction presents the context of the report and draws the main lines of questioning – namely, what the purchase of Hacking Team's software implies for Latin American democracies, how the software is utilized, its reach and potential dangers, whether its use is legal or not and whether or not there are sanctions in the second case. Two parts made up by five chapters focus, first, on the details about the human and technical aspects of how the RCS works. Secondly, on the ethical and legal issues around the use of unregulated surveillance and communication interception technologies by nation states. The work's conclusion states that the legal frameworks necessary to regulate the use of surveillance software by the police exist, but are outdated and should be enforced with greater care.

The report engages in two main discussions: the (in)security of information, especially with regard to controlling the sale and trafficking of so called "dual use technologies" (which can have both a civilian and military purpose) - in this case Latin American States' use of proprietary hacking tools to spy on the population; and the region's legal frameworks surrounding the respect for digital human rights, particularly concerning the right to privacy, freedom of speech and due process.

The overall analysis of the report focuses strongly on the second discussion by bringing forward the discrepancies between the use of spying software and the protection that the legal frameworks of each of the referred Latin American countries should provide. It analyzes the legality of using RCS through three lines of questioning: 1) in the context of judicial investigations or the activities of intelligence organizations; 2) with regard to the rules and regulations that allow geolocalization of people through their devices; 3) as compared to the use of search warrants. In this sense, the report shows a markedly normative character that seeks to put forward the illegality of producing, purchasing and using hacking/spying software. More specifically, it argues that even though interception of private communications is regulated in all of the alluded countries, RCS escapes judicial order not only because it is much more invasive than traditional surveillance techniques, but because its features are hardly contemplated by the letter of the law. Thus, its use jeopardizes the right to privacy, freedom of speech and – especially – to due process.

Ultimately, the report pushes for an open discussion to draw out the adequate norms, legal regimes and sanctions that have to regulate these technologies. It also states that intelligence services, which have far greater legal leeway to spy on the population, should be bound by a framework that specifies well-defined controls and responsibilities, clearly established capacities and application parameters, transparent and openly discussed criteria to decide who might be a "suspect" or whose devices can be spied on.

The report is interesting in many respects; its strongest suit is the detailed legal overview it makes for each of the alluded Latin American countries. Another strong point is that it evidences a growing strategy for mass State surveillance of the public – namely, the hacking of personal electronic devices - and puts a strong emphasis on the extent to which it can be detrimental to any individual. It exploits primary sources that are very rich and seldom used and gives salience to hacking, leaking and information (in)security. However, it is not devoid of problems.

The main concern is the overall normative approach that it presents. Not only does it rely too heavily on the letter of the law to make its assertions and fails to provide and analyze concrete examples of the use of RCS, but, more importantly, it is completely oblivious to the existence of a very broad information security community that incarnates the "civilian side" of these "dual use technologies". A very active community that develops, uses and analyzes both proprietary and free and open source software for penetration testing and signals' intelligence, and that constantly spurs debate and exposes the (in)security of information against the backdrop of a worldwide market that feeds from it, as well as against overbearing State espionage.