THE POLITICS OF SURVEILLANCE

Political opponents and activists are among those monitored in Latin America. **Katitza Rodríguez** charts the erosion of privacy in the region

While most Latin American countries have democratically-elected governments, many still fail to respect human rights, including the right to privacy. Across the region, there have been multiple scandals involving government officials and intelligence agencies engaged in illegal surveillance of communications. These include numerous chilling examples of how interception technologies are being misused to spy on politicians, dissidents, judges, human rights organisations and activists. Although privacy violations vary from country to country, and the full extent of government surveillance in the region remains largely unknown, newly disclosed data gathering programmes hint at the architecture of surveillance lying beneath the surface of ostensibly democratic societies.

These surveillance systems demonstrate how communication interception is being used as a political tool to identify, control and stifle dissent. Their use also highlights the lack of transparency and accountability that surrounds pervasive government surveillance in many Latin American countries. In 2009, Colombia's 'Las Chuzadas' scandal revealed that members of the country's intelligence service allegedly carried out illegal, widespread

Colombia's President Alvaro Uribe announces he's no longer allowing wiretapping by Colombia's domestic intelligence agency, 26 February 2009
Credit: Fernando Vergara/AP

surveillance and wiretapping of key politicians, judges, dissidents and human rights NGOs. Litigation about the surveillance is currently pending in the Colombian courts. In March 2011, the Inter-American Commission on Human Rights opened an investigation into the role of Colombian state officials in executing this mass surveillance programme.

Perhaps the most severe instance of widespread government surveillance took place in Peru during the presidency of Alberto Fujimori. Fujimori, who is currently in jail, was convicted of mass illegal surveillance of prominent Peruvian citizens. Peruvian prosecutors found that the former president devised and implemented 'Plan Emilio' to conduct nationwide surveillance of politicians, ministers, journalists and activists. In 2010, judicial authorities in Peru discovered a former naval intelligence employee illegally intercepted 52,947 emails from journalists and political opponents of the Fujimori government between 1999 and 2000. The case has yet to go to court.

Leaked US diplomatic cables posted on the WikiLeaks whistleblower website shed light on the US Drug Enforcement Administration's (DEA) communications surveillance programme and how the governments of Paraguay and Panama pressured the US government to allow the use of these technologies for operations unrelated to narcotics investigations. According to the cables, both countries sought US cooperation to expand their respective capacities to spy on mobile communications for political gain.

In Paraguay, this surveillance was undertaken ostensibly to deal with the threat of the leftist guerrilla group the Paraguayan People's Army. A diplomatic cable dated 18 February 2010 reveals that the DEA conducted an active mobile phone spying programme for counter-narcotics efforts in Paraguay beginning in 2009. The cables also reveal that the Paraguayan government requested access to the software used by the DEA to perform eavesdropping for other purposes. US diplomats even warned about the possibility that these surveillance technologies could be misused for unrestricted eavesdropping and political advantage:

> The ambassador made clear that the US had no interest in involving itself in the intercept programme if the potential existed for it to be abused for political gain, but confirmed US interest in cooperating on an intercept programme with safeguards, as long as it included counter-narcotics. While noting that the Interior Ministry's current personnel are trustworthy, the ambassador noted that others could abuse this technology in the future.

The US embassy repeatedly denied Paraguayan government requests for unrestricted access to its surveillance software. According to the US envoy, the interior minister of Paraguay disclosed that his government's 'top priority was capturing the [Paraguayan People's Army], which had to take precedence over counter-narcotics'. 'Counter-narcotics are important,' he said, 'but won't topple our government. The [Paraguayan People's Army] could.'

The cables also reveal the nature of 'cooperation' between US law enforcement and Paraguayan telecom companies, illustrating how the US influenced otherwise hesitant actors:

> TIGO (Millicom), one of Paraguay's leading cell phone providers, told the Ambassador that though they had concerns about the [Government of Paraguay's] decision to move forward with

an intercept programme, they felt that US involvement in the programme would provide them with some 'cover'.

Despite their misgivings, US embassy staff concluded that they could not refuse to cooperate indefinitely without threatening the DEA's broader agenda. 'Get on board or get left behind,' reads the sub-title of the cable. 'If we are not supportive,' the cable continues, 'the [Government of Paraguay] will view us as an obstacle to a key priority, which could jeopardise our broader relationship and the DEA's ability to pursue counter-narcotics leads … We have carefully navigated this very sensitive and politically sticky situation, and hope that we can move forward quickly in order to make the most of it.' In effect, the US government acknowledged its surveillance assistance would likely be misused for political surveillance, but continued to cooperate.

A similar dynamic played out in Panama. According to a leaked cable dated 22 August 2009, 'Panama 000639', the Panamanian government, headed by President Ricardo Martinelli, repeatedly requested technical assistance from the US to extend its wiretapping capacity. In July 2009, Martinelli sent a BlackBerry message to the ambassador that read, 'I need help with tapping phones.' Moreover, Martinelli sought the DEA's cooperation to acquire US government support for his politically-driven wiretap project. As embassy staff report in the cables, Martinelli thought it was unfair that the 'DEA collects information but that Panama does not benefit from that information'. In his communication with the embassy, he made reference to various groups and individuals he thought should be wiretapped and 'he clearly made no distinction between legitimate security targets and political enemies'. Martinelli went on to say that the US government 'should give the [Government of Panama] its own independent wiretap capability as "rent" in exchange for the use of [its] facilities'.

When the Panamanian government threatened to reduce its cooperation with the counter-narcotics surveillance programme, the US ambassador to Panama counter-threatened to inform his superiors in Washington DC: 'The ambassador forcefully defended the DEA program and pointed out that the jointly-investigated cases were taking criminals off of Panama's streets and making the country safer. … She would readily inform Washington [of his threat] and [everyone would see] Panama's reputation as a reliable partner plummet dramatically.'

Although Martinelli backed off, the Panamanian government subsequently confirmed that it could expand the wiretapping programme on its own, and had already met with the heads of Panama's four mobile phone operators to discuss methods for obtaining mobile call data. The US

Police outside the National Intelligence Service headquarters in Lima following the release of information about the government's illegal surveillance programme, 18 September 2000
Credit: Pilar Olivares/Reuters

ambassador encouraged the Panamanian government to 'streamline' its process for obtaining emergency court orders for lawful interception, but expressed concerns in another cable about political pressure undermining the independence of the judiciary. According to the cables, Martinelli 'chided' the ambassador's advice for being 'too legal'.

US government officials defended their own wiretap programme in the cables, stating, '[it] works well and upholds the rule of law [and] would easily withstand public scrutiny were it to come to light'. In its coordination with Panamanian authorities to meet US government collection requirements, officials cautioned 'against the danger of local officials trying to commandeer the program for internal political games' and attempted to 'only conduct limited law enforcement wiretap programs in cooperation with Panamanian law enforcement and judicial authorities, directed only against genuine law enforcement targets, in a process managed by a Panamanian prosecutor and

approved by a Panamanian Supreme Court judge'. The effectiveness of legal safeguards against interception of communications depends on government compliance with national law. This disclosure shows why we cannot assume that governments will always comply.

Another cable, dated 24 December 2009, reveals that the US decision to remove the DEA's Matador wiretap programme from Panamanian government control was met with resistance and more threats, citing 'a series of obstacles, including threats from the Council for Public Security and National Defense director to expel the DEA from Panama and restrict payments to vetted units and generally weak support for the move from Martinelli and senior [government] leaders'. The US ambassador added that the embassy remained concerned about ongoing efforts by the Panamanian government to weaken judicial controls over domestic surveillance and undermine civil liberties at a time when Panama's judicial institutions were under assault by the executive branch.

'With Panama's notoriously corrupt judicial system (rated 103 out of 133 by the World Economic Forum),' it stated, 'We are not confident that the new judge will uphold the same standards and civil liberties protections that the Panama supreme court has exercised in its oversight of Matador to date.' The ambassador warned his colleagues that the DEA surveillance system should not be used to compromise democratic values in the name of security.

The ambassador concluded by urging the US government not to get entangled in politically motivated wiretapping, advising against involvement in 'questionable activities' in Panama. 'The recent [Las Chuzadas] scandal in Colombia illustrates the catastrophic consequences of politically motivated wiretaps,' he wrote, 'and such a scenario could easily unfold in Panama if the government of Paraguay continues its present course of action. If we cannot guarantee with a high level of confidence that the Matador program will not be misused for political purposes, then we prefer to suspend the program.' Clearly, the ambassador understood the potential dangers posed by the misuse of DEA surveillance systems and how they could be used to undermine free expression and other democratic principles promoted by US policy.

State surveillance can also be achieved through real name registration requirements for the purchase of a mobile phone or SIM card activation. In several countries, there is an emerging trend towards eliminating anonymous communication. Peru, Brazil and Mexico have adopted regulations that compel telecommunications companies to collect and identify pre-paid mobile users' contact information for later potential use by law enforcement entities. A similar bill is being discussed in Guatemala. These measures seek

to facilitate the identification of criminals and address the alleged threat to security created by the type of mobile phone account that does not require registration or the collection of detailed personal information.

These registration regimes strike a heavy blow against anonymous communications; citizens not suspected of any crime are denied the use of anonymous pre-paid cell phones to communicate. In some countries like Peru and Brazil, these identification requirements have been extended to cyber cafes, the medium in which a significant proportion of the population with low incomes accesses the internet.

To obtain a mobile phone number in Mexico, citizens are required to provide proof of their current address, present the unique identity code given to both citizens and residents of Mexico, produce valid photo identification, and submit to fingerprint scanning. In accordance with the law, Mexican mobile phone companies are responsible for encouraging the users of their 80m devices to register with the National Registry of Mobile Phone Users. In April 2011, Salvador Guerrero, an authority at the Institute for Access to Public Information of the Federal District, criticised the National Register of Mobile Phone Users for failing to protect the personal data of Mexican citizens: 'During the past year it has become clear that the [registry] is not capable of complying with the function for which it was designed and that is to prevent extortion and kidnapping, the latter figure increasing by eight per cent in 2010 compared to 2009.'

In a few countries, registration requirements are being extended beyond mobiles to internet cafes. In Peru, internet cafes are compelled to register the users of their facilities. Brazil adopted a similar measure in April 2011. The sponsor of the Brazilian legislation, Representative Alex Sandro, said of the measure, 'It will be like the pre-paid phone, which established a registry for the purchase [of pre-paid phones], and the crimes that were committed on these devices still exist, but will decrease greatly because of the possibility of screening.' But this mandate violates the right to speak anonymously, and hinders its crucial function in people's political and social discourse.

People should be able to use the internet anonymously to share sensitive information and express unpopular or controversial opinions without fear of retaliation. The tendency to associate anonymity with criminality by some government officials and law enforcement agencies is troubling. Anonymity is necessary for citizens engaged in legitimate opposition to government policies and for whistleblowers who leak information that those in power would prefer to erase. It is also critical for victims of violence, those who have experienced discrimination because of HIV/Aids, dissidents, homosexuals and survivors of abuse.

Almost all Latin American countries protect the right to privacy in their constitutions, and a number of countries have signed and/or ratified the UN International Covenant on Civil and Political Rights. But many countries have not yet enacted comprehensive legislation to protect individuals' personal data, with the exception of Argentina, Mexico, Chile and Uruguay. Others (including Brazil, Bolivia, Colombia, Costa Rica, Guatemala and Peru) are currently considering enacting a comprehensive data protection law, or are updating their weak legal safeguards, as in the case of Chile. Governments' demands for the collection and storage of more information, including biometric data in national identification cards or passports, jeopardises individuals' privacy and security, creating a database that has the potential to locate and track people with a high degree of accuracy. Plans for these sorts of databases are currently underway in several countries. A serious discussion is needed about the policy implications of covert surveillance programmes in Latin America and their impact on citizens' privacy and freedom of expression rights. ❐

40(2): 116/123
DOI: 10.1177/0306422011411270
www.indexoncensorship.org

Katitza Rodríguez is the international rights director at the Electronic Frontier Foundation