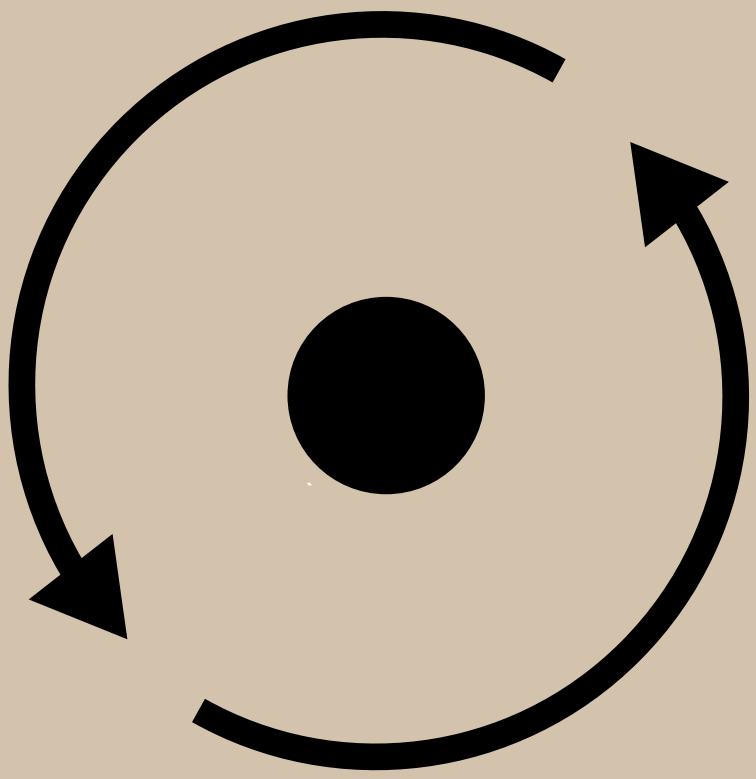
PRIVACY INTERNATIONAL

Demand/Supply: Exposing the Surveillance Industry in Colombia

Special Report



Demand/Supply: Exposing the Surveillance Industry in Colombia

XXXXXXXXXXXX
September 2015

PRIVACY INTERNATIONAL

www.privacyinternational.org



Bogotá skyline from Monserrate mountain.
Credit - Privacy International (2014)

Table of Contents

List of Acronyms	6
Executive Summary	7
Recommendations	9
The Colombian Surveillance State	11
Selling Surveillance	17
Network Interception	22
The Companies: Network Interception	25
Tactical Surveillance	35
Conclusion	41
Annex	42

List of Acronyms

3G	Third generation mobile telecommunications technology
4G	Fourth generation mobile telecommunications technology
ASFADDES	Association for the Relatives of the Detained-Disappeared
CALEA	US Communications Assistance for Law Enforcement Act
CCAJAR	The José Alvear Restrepo Lawyers' Collective
CIA	US Central Intelligence Agency
DANE	National Bureau of Statistics
DAS	Administrative Security Department
DEA	US Drugs Enforcement Agency
DIJIN	Directorate of Criminal Investigation and Interpol
DIPOL	Directorate of Police Intelligence
E1	Telecommunications link designed to carry voice and data communications
ELN	National Liberation Army
Esperanza	Interception platform managed by Fiscalía
ETSI	European Telecommunications Standards Institute
FARC	Revolutionary Armed Forces of Colombia
Fiscalía	Office of the Attorney General of Colombia
GAULA	Unified Action Groups for Personal Liberty
GPS	Global Positioning System
GSM	Global System for Mobile Communications
IMEI	International Mobile Station Equipment Identity
IMSI	International Mobile Subscriber Identity
IP	internet protocol
IRS	'Integrated Digital Recording System', communications surveillance system managed by DIPOL
ISP	Internet Service Provider
MINTIC	Ministry of Information Technology and Communications
MSC	Mobile switching centre
OEM	Original equipment manufacturer
PGP	Pretty Good Privacy, data encryption program
PUMA	Single Monitoring and Analysis Platform, communications surveillance system managed by DIJIN
RCS	Remote Control System, surveillance solution by Hacking Team
TAP	Traffic Access Point
TMSI	Temporary Mobile Subscriber Identity
TSP	Telecommunications Service Provider

Executive Summary

The global surveillance industry comprises an expanding group of companies, small and large, that sell surveillance technologies primarily to law enforcement and intelligence agencies around the world. In recent years, the industry has come under heightened scrutiny and attack for its impact on human rights and its role in equipping repressive regimes with tools of oppression. In addition, the media's coverage of the use and abuse of surveillance technologies by governments against activists, journalists, dissidents and ordinary citizens has surged in recent years. Yet much more remains to be understood about the surveillance industry.

The commercial surveillance industry is relatively new. Historically, the private sector played a limited role in providing the surveillance capabilities used by state law enforcement and intelligence agencies. Especially in the realm of intelligence gathering, states by and large preserved a monopoly on the development and deployment of surveillance technologies as surveillance was a time- and resource-intensive activity that required a significant financial commitment.

The picture has shifted significantly in the past few decades. New technologies have put the collection and retention of vast amounts of data within the budgetary reach of more and more governments. Concurrently, a commercial industry has emerged to service states' desire for ever-more expansive surveillance capabilities. The surveillance industry was estimated to be worth around US$ 5 billion in 2011 and is growing by 20 per cent annually.[1] The dominant narrative presented in companies' marketing materials is one in which they are part of a legitimate and responsible industry whose primary purpose is to protect human security by providing surveillance technologies to government actors. These technologies are meant to ward against the looming threat of increasing criminality facilitated by modern communications infrastructure.

However, surveillance technologies can also be used by governments to target opponents, crack down on dissent, intimidate populations, chill expression and destroy the possibility of private life. These technologies can also serve to subject entire populations to indiscriminate monitoring. In short, they can become part of a broader state apparatus of oppression.

The companies that sell surveillance technologies often enable and facilitate state surveillance in violation of human rights standards, yet the legal and ethical implications of their actions and the technologies they sell have never been sufficiently scrutinised. This series, Demand/Supply: Exposing the Surveillance

1 "Spies Fail to Escape Spyware in $5 Billion Bazaar for Cyber Arms", Bloomberg News, 22 December 2011, http://www.bloomberg.com/news/2011-12-22/spies-fail-to-escape-spyware-in-5-billion-bazaar-for-cyber-arms.html

Industry in Colombia, aims to demonstrate the private sector's role in equipping government agencies with surveillance tools. Its focus is the industry's role in designing, marketing and deploying invasive surveillance systems; the lack of transparency around capacities and product flows; and the absence of adequate human rights due diligence processes and accountability mechanisms.

This report concerns Colombia where the government has been fighting an armed insurgency for over 50 years. Various law enforcement agencies, from the Administrative Department of Security (Departamento Administrativo de Seguridad, DAS) to the Police Intelligence Directorate (Dirección de Inteligencia Policial, DIPOL) have been implicated in the unlawful targeted surveillance of journalists, activists and government actors. The Army, too, has set up interception rooms to spy upon peace negotiations and influence electoral processes. Privacy International's recent report Shadow state: surveillance, law and order in Colombia details the types of surveillance technologies used by Colombian law enforcement and intelligence agencies. The report exposes the efforts of the Colombian state, specifically the Police, to build a shadow mass surveillance system in the absence of clear lawful authority, safeguards against abuse and opportunities for public scrutiny.

Over the past decade, the Colombian government has primarily looked to private companies locally, as well as companies in the UK, the US and Israel to supply surveillance equipment. These companies have provided technologies that enable both network surveillance (the monitoring of communications data and content from service providers' networks) and tactical surveillance (the monitoring of communications data and content wirelessly or from target devices).

We begin by describing the state of surveillance in Colombia and the law enforcement and intelligence agencies implicated in it. We then provide a broad overview of the surveillance technology market in Colombia, and describe the types of technologies being sold to Colombia and the companies selling them. We conclude by discussing the legal and ethical responsibilities of the companies equipping the Colombian state.

Recommendations

To foreign governments and export control authorities:

- Adopt legislation making financial or technical assistance, transfer of equipment, or sharing of intelligence to/with law enforcement, military, or intelligence agencies in foreign countries conditional on strong human rights provisions.
  Such provisions must explicitly prohibit any support for individuals or agencies proven or strongly suspected to be involved in human rights violations.
- Carry out an extensive audit of the security assistance that has been provided to Colombian law enforcement, military, or intelligence agencies since 2000 to ascertain if any such assistance has led to human rights violations.
- Publicly disclose all forms of security assistance to Colombia, including details regarding financial or technical assistance, transfer of equipment, or sharing of intelligence with law enforcement, military or intelligence agencies.
- Adopt strong end-use monitoring mechanisms regarding security assistance provided to foreign countries via, but not limited to, diplomatic channels and engagement with civil society and multilateral institutions.
- Publicly disclose any such end-use monitoring mechanisms and publish, on an annual basis, the results of any such monitoring of security assistance.
- Adopt domestic legal mechanisms by which parliamentarians and citizens can challenge the provision of security assistance to a foreign country if such provision has contributed to or may contribute to human rights violations.
- Do not approve export-controlled surveillance technologies where there is a risk they will be used to facilitate internal repression or to otherwise undermine human rights, or if there is no clear legal framework governing the exported items' uses.
- Commit to and implement agreements on export control measures related to electronic surveillance technologies. While some measures have already been taken following recent changes to the Wassenaar Arrangement, this does not preclude national governments and regional institutions such as the European Union from pursuing unilateral regulations.
- Identify products that can be subjected to export licensing without harming security research or otherwise negatively impacting the development of the information and communication technology sector. A possible solution could include not just the addition of a product to a national or multilateral export control regime control list, but also end-use and end-user stipulations.
- Ensure strong human rights criteria are included in export control provisions that are specific to surveillance technologies. Human rights criteria should take into account the receiving state's legal framework, oversight mechanisms, and respect for international human rights standards, and the end-user's

record regarding the use of electronic surveillance.
- Work within export control regimes and with multilateral institutions and other states to identify and mitigate challenges to applying and enforcing export control regulations on surveillance technologies, particularly regarding brokering, re-export, incorporation, and diversion challenges.

To foreign and domestic companies selling communications surveillance equipment:

- Carry out due diligence research on any potential beneficial end-users prior to agreeing to a potential transaction.
- Do not sell or provide a surveillance product if the beneficial end-user of the product cannot be clearly identified or presents a documented record of human rights abuse that is likely to be enabled/ by the product.
- Do not sell or provide a product to a client if there is no clear legal framework or oversight mechanism governing its use within the country of destination.
- Stipulate clear end-use assurances in contractual agreements with customers encompassing strong human rights safeguards and protecting against their arbitrary and unlawful use.
- Carry out a periodic review and refuse to carry out maintenance, training, or updates if the end-use does not conform to these contractual obligations.
- Develop internal policies relating to re-sellers and distributors, and include provisions in contractual agreements ensuring their adherence to export control regulations and to the developer's own human rights provisions.
- Original Equipment Manufacturers (OEMs) should ensure that the company incorporating their equipment adheres to export control regulations and to the OEM's own human rights provisions.
- Commit to and publish strong Corporate Social Responsibility (CSR) commitments conforming to the United Nations' Guiding Principles on Business and Human Rights' in relation to 'human rights'.
- Initiate an annual review of adherence to CSR commitments and international human rights standards and publish its outcomes. Included within this should be strong transparency measures containing, to the greatest extent possible, a list of end-users.

The Colombian Surveillance State

The interception of private communications is a legitimate state activity and an acceptable constraint on individuals' right to privacy when performed in accordance with a clear, detailed legal framework; in pursuit of a legitimate aim; and in a manner proportionate to that aim. States can build and deploy communications surveillance architecture in a manner consistent with international human rights standards provided they do so in a context in which surveillance powers are clearly legislated for and overseen, and that those who are exercising surveillance powers are transparent and accountable to the public.

Colombian law enforcement and intelligence agencies' surveillance capabilities have grown with the expansion of military operations against the country's largest guerrilla group, the Revolutionary Armed Forces of Colombia (FARC), and its smaller cousin, the National Liberation Army (ELN).[2] The Colombian armed conflict is the longest-running of its kind in the Western Hemisphere and has for more than fifty years involved a number of actors.

The other main actor, paramilitary groups, which sometimes worked in tandem with parts of the state, officially demobilised in the mid-2000s. Several other leftist guerrilla groups also demobilised at various stages of the conflict. The conflict has claimed the lives of nearly 220,000 people,[3] most of them civilians. In the period 1985-2012, 5.7 million people were internally displaced[4] and at least 25,000 people were forcibly disappeared.[5]

Accounts of the illegal interception of private communications pervade accounts of extrajudicial disappearances and killings. Different agencies have been involved in these illegal interceptions. In one famous case in 2002, more than 2,000 phone lines were illegally tapped by the joint military-police Unified Action Groups for Personal Liberty (Grupos de Acción Unificada por la Libertad Personal, GAULA), according to the Office of the Attorney General of Colombia (Fiscalía).[6] Among those targeted were a group representing families of the disappeared, the Association for the

2 The US State Department has listed both groups on its Foreign Terrorist Organizations list. 2015. http://www.state.gov/j/ct/rls/other/des/123085.htm

3 "Report says 220,000 died in Colombia conflict", Al Jazeera, 25 July 2013, http://www.aljazeera.com/news/americas/2013/07/201372511122146399.html

4 "2015 UNHCR country operations profile – Colombia", UNHCR, 2015, http://www.unhcr.org/pages/49e492ad6.html

5 "NGO's remember 25,000 forcibly disappeared in Colombia, call on govt to do more", Colombia Reports, 22 May 2014, http://colombiareports.co/ngos-organize-commemoration-week-25000-forcibly-disappeared-colombia/

6 "Informe sobre Derechos Humanos: Colombia", US Department of State, 4 March 2002, http://www.acnur.org/t3/uploads/media/COI_53.pdf

Relatives of the Detained-Disappeared (ASFADDES), a group that had seen at least two of its own members disappeared in the same year. In 2007, eleven police generals from DIPOL were dismissed following revelations that the agency had tapped the phone lines of influential opposition politicians, journalists, lawyers and activists.[7] In 2014, the Colombian weekly magazine Semana alleged that a Colombia army unit codenamed Andromeda had been spying for more than a year on the Government's negotiating team in ongoing peace talks with the FARC guerrillas.[8]

Yet the most notorious of the surveillance scandals involves the Administrative Security Department (Departamento Administrativo de Seguridad, DAS). Special strategic intelligence groups of the DAS conducted targeted surveillance of an estimated 600[9] public figures including parliamentarians, journalists, human rights activists, lawyers, and judges, among others. The story was broken by Semana in February 2009.

Profile

DAS

Founded in 1953, the Administrative Department of Security (Departamento Administrativo de Seguridad) was one of Colombia's security services formally mandated to produce intelligence required by the government as a tool for decision-making and policy formulation related to internal and external state security.[10] It was dissolved in October 2011 following revelations it intimidated and illegally wiretapped Supreme Court judges, human rights workers, journalists and opposition politicians and supported violent paramilitary groups.

The scale of intimidation carried out against these persons by the DAS was extensive. The role of communications surveillance was of great strategic importance. The DAS intercepted phone calls, email traffic and international and national contacts lists, using this information to compile psychological profiles of targets and conduct physical surveillance of subjects and their families, including children, according to files retrieved during an investigation by the Fiscalía[11]. The DAS targeted the

7 "El DAS-gate y las 'chuzadas', vuelve y juega", El Espectador, 21 February 2009, http://www.elespectador.com/impreso/judicial/articuloimpreso120201-el-das-gate-y-chuzadas-vuelve-y-juega

8 "¿Alguien espió a los negociadores de La Habana?" Semana, 3 February 2014, http://www.semana.com/nacion/articulo/alguien-espio-los-negociadores-de-la-habana/376076-3

9 "Más de 600 personas habrían sido 'chuzadas' ilegalmente por el DAS, según investigadores", Caracol Radio, 17 April 2009, http://www.caracol.com.co/noticias/judiciales/mas-de-600-personas-habrian-sido-chuzadas-ilegalmente-por-el-das-segun-investigadores/20090417/nota/446294.aspx

10 Decree 218 15 of February 2000, Government of Colombia, 15 February 2000, https://www.oas.org/dil/Migrants/Colombia/Decreto%20N°%20218%20del%2015-02-2000.pdf

11 Un 'manual' para seguir y acosar a personas calificadas como opositores tenía el DAS", El Tiempo, 13 June 2009, http://www.eltiempo.com/archivo/documento/CMS-5436047

journalist Hollman Morris. Threats forced him into exile on several occasions. Claudia Duque, a lawyer and journalist formerly working with the José Alvear Restrepo Lawyers' Collective (CCAJAR) survived kidnapping attempts and received graphically violent phone threats. The DAS files about Duque contained extensive evidence of communications and physical surveillance[12]. Such was the scale of the illegal interception that seven Supreme Court justices were recused from the 2011 trial of the former DAS head because even they were reportedly victims.[13] The scandal-ridden DAS was disbanded in October 2011. Its workforce was assigned elsewhere, including to the Fiscalía, which was charged with investigating the DAS abuses. The head of the DAS in 2008, Maria del Pilar Hurtado was convicted for illegal surveillance, in February 2015.[14] Yet the spectre of illegal interception of communications and the abuses of surveillance laws still hangs over the Colombian state.

12 Former security operatives charged in journalist's torture in Colombia", IFEX, 18 March 2013, https://www.ifex.org/colombia/2013/03/18/security_charged/ and "Colombian official convicted of 'psychological torture' of journalist", Committee to Protect Journalists, 22 December 2014, https://cpj.org/2014/12/colombian-official-convicted-of-psychological-tort.php

13 "7 judges withdrawn from wiretap trial", Colombia Reports, 12 August 2011, http://colombiareports.com/7-supreme-court-judges-victimized-in-wiretap-scandal-withdrawn-from-trial/

14 "'Chuzadas' del DAS: crimen y castigo", Semana, 28 February 2015, http://www.semana.com/nacion/articulo/chuzadas-del-das-crimen-castigo/419365-3

Since the late 1990s, the lawful interception of communications on Colombian networks has been effected through Esperanza – an interception system managed by the Fiscalía, and accessed by Police and formerly the DAS for the purpose of judicial prosecution on a case-by-case basis.

Esperanza functions as a targeted interception system that relies on requests by human users, the Fiscalía administrators, to 'task' Colombia's service providers to send specifically requested audio and data records for mobile phone and fixed-line calls. Use of Esperanza is governed by the Colombian Constitution and Criminal Procedural Code, both of which lay out in considerable detail the circumscribed powers of the Fiscalía to lawfully intercept private communications.

Profile

FISCALIA

The Office of the Attorney General (Fiscalía General de la Nación) is an entity of the judicial branch of government with full administrative and budgetary autonomy with responsibility for the effective administration of justice.[15] Established in 1991, it is mandated to carry out criminal investigations for the purpose of judicial prosecution, to ensure the protection of victims and witnesses, and to direct and coordinate the functions of the judicial police. The Fiscalía is responsible for administering the Esperanza platform, reviewing and approving interception orders from other agencies including the DAS and the Police. The Fiscalía leads the ongoing investigation into the DAS' illegal surveillance in the mid-2000s, reportedly by abusing access privileges to the Esperanza platform.

In recent years, communications interception capacity has expanded to include mass, automated interception of phone and email traffic on the backbone of the nation's telecommunications infrastructure. This amounts to mass surveillance. Millions of people's communications are potentially swept up, filtered, monitored and analysed before being stored for further interrogation or deleted, even if those people are not suspected of any wrongdoing. Unlike traditional forms of targeted surveillance, automated interception allows for whole cables to be intercepted en masse by placing a probe directly on the cable. Components of the system sort, store, repackage and reassemble intercepted data according to how they are programmed.

The Single Monitoring and Analysis Platform (Plataforma Única de Monitoreo y Análisis, PUMA) was launched in 2007 as a 'monitoring' system administered and paid for by Police and managed by DIJIN. The technology on which it is built allows for massive, passive, untargeted interception of Colombians' communications.

15 ¿Quiénes somos?", Fiscalía, 2015, http://www.fiscalia.gov.co/colombia/la-entidad/quienes-somos/

Profile

DIJIN

The Directorate of Criminal Investigation and Interpol (Dirección de Investigación Criminal e Interpol) is the police directorate in charge of judicial investigation. It is one of eight police Directorates accountable to the General Directorate under the Ministry of Defence. Its role is to support criminal investigation in technical, scientific and operational areas, of its own initiative or according to orders from the Fiscalía. DIJIN officers have lent forensic expertise to the investigations of illegal interceptions.

DIPOL also manages a system that intercepts vast volumes of communications signals as well as non-communications data via network probes connected to a monitoring centre platform. Monitoring centres receive, process and retain data collected by a variety of data sources, including internet monitoring, location monitoring, phone monitoring, and audio and video surveillance. Once collected, this data is analysed by powerful computer programmes that display connections between people. By linking people and their contacts and those persons' contacts, analysts can build profiles of individuals and their contacts and access their private communications based solely on their communication patterns. Depending on how the components of the technology are programmed, all of this analysis can take place before a human even looks at the intercepted data.

Profile

DIPOL

Police Intelligence Directorate (Dirección de Inteligencia Policial, DIPOL) is the police directorate responsible for producing strategic and operational intelligence related to disturbances in public order, security and defence. It is mandated to conduct national counterintelligence activities.[16] It is one of eight Police directorates accountable to the General Directorate under the Ministry of Defence. DIPOL is also responsible for leading technological development plans with regard to intelligence activities within the Police. DIPOL officers have been accused of illegal surveillance against journalists.[17]

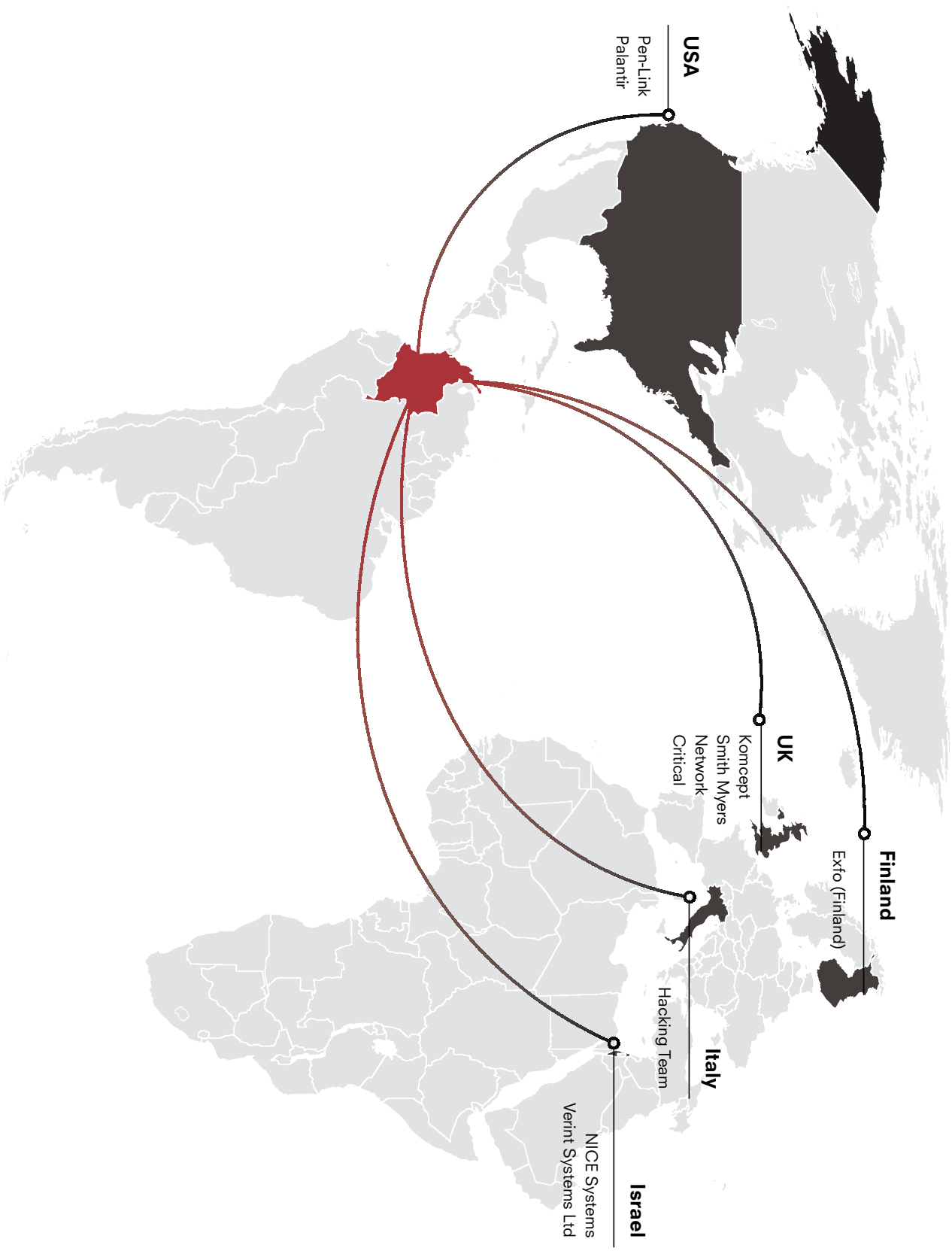
16 "Dirección de Inteligencia Policial", Colombia National Police, 2015, http://oasportal.policia.gov.co/portal/page/portal/UNIDADES_POLICIALES/Direcciones_tipo_Operativas/Direccion_Central_Inteligencia

17 "Senior intelligence chiefs suspended or resign over scandal on tapping of journalists' and politicians' telephones", IFEX, 2 July 2007, http://www.ifex.org/colombia/2007/07/06/senior_intelligence_chiefs_suspended/

In 2012, DIPOL also negotiated the purchase of powerful open source intelligence technology that would have allowed it to build on their existing platform to analyse and process vast amounts of data and communications, from Facebook interactions to biometric details, and to draw conclusions about the likelihood, however faint, of individuals' involvement in past or future criminal activities. In addition, the Police acquired intrusion software, which would enable targeted remote exploitation – in essence, hacking and control – of individuals' devices. Such technology provides the user, in this case, the Police, with extraordinary capacities, such as remotely turning on the microphone and camera of a target's phone or computer – seeing and hearing everything in the vicinity of the device.

The State agencies acquiring these capabilities are doing so not only outside of public scrutiny, but also without legal sanction. None of the above listed agencies are authorized to conduct 'interception' without the oversight of the Fiscalía. The Constitution and Criminal Procedure Code provide that the interception of communications can only be effected through the Fiscalía, in the presence of a judicial investigation, on a targeted basis. The Colombian legal framework governing communications surveillance suffers from fatal technical and legal errors examined at length in Privacy International's report, Shadow State: surveillance, law and order in Colombia.

Selling Surveillance



A selection of companies whose surveillance products have been sold to Colombian law enforcement and intelligence agencies.

The Colombian government has purchased a significant quantity of communications surveillance equipment. Most of this is supplied by foreign companies through Colombian partners.

Financing for surveillance technology ballooned with the joint US-Colombia 'Plan Colombia' military assistance program developed in the late 1990s. The military is particularly well funded. The 2015 Colombian defence budget was US$ 14.17 billion.[18]

Colombia both hosts and attends a number of surveillance and security technology trade shows. Intelligence Support Systems World (ISS World), also known as the 'Wiretappers' Ball' is one of the largest trade shows and focuses on North American and European providers. The Colombian police attended ISS World in 2012 where three Colombian companies exhibited their products: Biotekne SAS, Colombia ASOTO Technology Group, and supplier to the Fiscalia for their Esperanza surveillance system STAR Colombia Inteligencia & Tecnología (STAR). [19] The annual Cibercolombia trade show and conference where primarily Israeli surveillance products are displayed are sponsored by the Israeli embassy in Bogotá. [20]

Much of the security equipment in Colombia is provided by international, especially American, companies. Over the past decade, the American funds, equipment and training supplied to elite units of the Colombian intelligence services were reportedly used to spy on Supreme Court justices, then-President Alvaro Uribe's political opponents and civil society groups. Intercepted communications were vital to covert Colombian and US Central Intelligence Agency (CIA) operations against the FARC.[21] While Colombian contracting law (Ley 80 de 1993) accords priority to security and national defence products made in Colombia by local manufacturers,[22] the National Treatment caveat of the 2006 United States-Colombia Bilateral Trade Agreement allows American companies to be treated as locals when they participate on public bids.[23] Israel is also a significant military supplier. Israeli-American company Verint Systems provided critical interception infrastructure used by the DAS, DIPOL and DIJIN from at least 2005. Verint Systems Ltd, is the Israeli sister company to US-headquartered Verint Systems Inc.

18 "Crunching the numbers on Colombia's 2015 budget", Colombia Reports, 26 August 2014, http://colombiareports.co/crunching-numbers-colombias-2015-budget/

19 "Program Schedule for Year 2013", ISS World, 2012, https://www.wikileaks.org/spyfiles/docs/ISS-2013-Sche2013-en.pdf

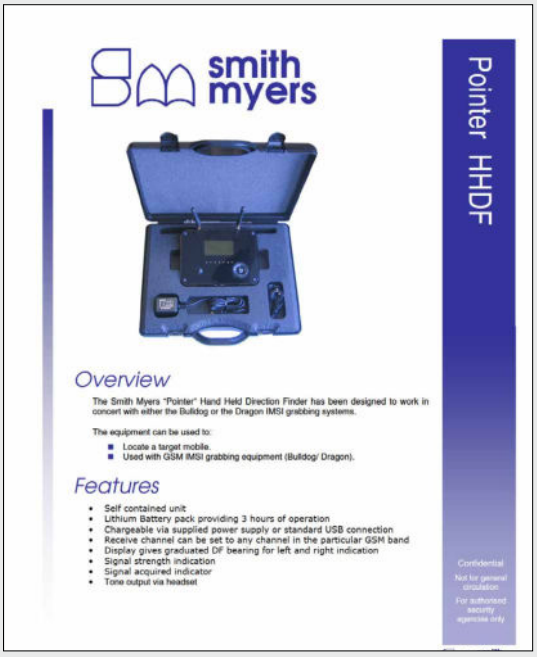
20 "Conference Ciber Colombia 2015", Israel Export Institute, 2015, http://www.export.gov.il/heb/Branches/Technologies/DefenceIndustries/Events/events,1418

21 "U.S. aid implicated in abuses of power in Colombia", The Washington Post, 20 August 2011, http://www.washingtonpost.com/national/national-security/us-aid-implicated-in-abuses-of-power-in-colombia/2011/06/21/gIQABrZpSJ_story.html

22 Decree 734 of 2012, Government of Colombia, 13 April 2012, http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=46940#0

23 "Chapter Nine: Government Procurement", Office of the United States Trade Representative, 2006, http://www.ustr.gov/sites/default/files/uploads/agreements/fta/colombia/asset_upload_file739_10140.pdf





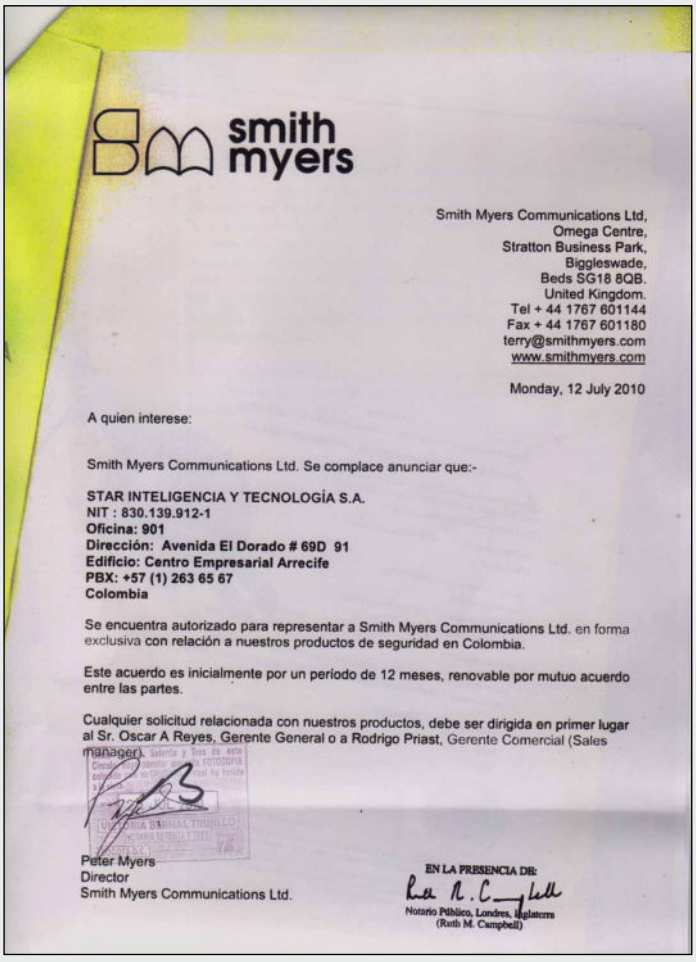


SPOILED FOR CHOICE

A small selection of tactical surveillance products on sale in Colombia: a credit card recording device by Swiss company Nagra; ‘Pointer’, a hand-held direction finder to be used while intercepting phone calls with an IMSI catcher by UK company Smith Myers Communications; and a video and audio recording device modelled on a baby seat by UK company LMW Electronics.

The types of surveillance products purchased by Colombian agencies from the private sector generally fall into two categories – those required for network surveillance and those that facilitate tactical surveillance. Typically, the Colombian government purchases the network probes and monitoring centres necessary for a network interception programme from large international vendors via Colombian companies who have exclusivity agreements to distribute specific international vendors' products, or who legally represent them in direct contracts with government clients.

Such partnerships include for example, those between Verint Systems and Compañía Commercial Curacao de Colombia (La Curacao); US company DreamHammer, represented in Colombia by Emerging Technologies Corporation;[24] UK company



smith myers

Smith Myers Communications Ltd,
Omega Centre,
Stratton Business Park,
Biggleswade,
Beds SG18 8QB.
United Kingdom.
Tel + 44 1767 601144
Fax + 44 1767 601180
terry@smithmyers.com
www.smithmyers.com

Monday, 12 July 2010

A quien interese:

Smith Myers Communications Ltd. Se complace anunciar que:-

STAR INTELIGENCIA Y TECNOLOGÍA S.A.
NIT : 830.139.912-1
Oficina: 901
Dirección: Avenida El Dorado # 69D 91
Edificio: Centro Empresarial Arrecife
PBX: +57 (1) 263 65 67
Colombia

Se encuentra autorizado para representar a Smith Myers Communications Ltd. en forma exclusiva con relación a nuestros productos de seguridad en Colombia.

Este acuerdo es inicialmente por un periodo de 12 meses, renovable por mutuo acuerdo entre las partes.

Cualquier solicitud relacionada con nuestros productos, debe ser dirigida en primer lugar al Sr. Oscar A Reyes, Gerente General o a Rodrigo Priast, Gerente Comercial (Sales manager).

Peter Myers
Director
Smith Myers Communications Ltd.

EN LA PRESENCIA DE:
Notario Público, Londres, Inglaterra
(Ruth M. Campbell)

DOING BUSINESS

Foreign surveillance companies conduct business in Colombia through local firms with whom they have exclusivity agreements, such as this one between Smith Myers Communications and STAR from 2010.

24 "DreamHammer Signs Drone Software Distribution Deal to Service Colombian Government Through Partner, Emerging Technologies Corporation", Business Wire, 15 May 2014, http://www.businesswire.com/news/home/20140515006450/en/DreamHammer-Signs-Drone-Software-Distribution-Deal-Service#.VM9YFId3aT8

Smith Myers Communications, represented by STAR in 2010; and US company Harris and Canadian company Allen-Vanguard, both of whom are represented by Eagle Commercial SA in 2006.[25] Local Colombian companies will often be loaned equipment from international providers to use in demonstrations with prospective government clients.

Another common way of responding to bids is for two or more Colombian companies representing international firms to form a 'temporary union' (unión temporal) to best respond to bids' technical requirements. These unions are often dissolved at the end of the contract. Other companies bidding in Colombia, like German firm Rohde & Schwarz, create legally separate Colombian subsidiaries.

With a few exceptions, Colombian companies do not produce the equipment necessary for network surveillance domestically. However, simple components of surveillance systems, such as closed-circuit television (CCTV) monitoring consoles and the screens and computers on which intercepted information is analysed, are manufactured locally. Some integrate their own tactical interception systems, such as Emerging Technologies Corporation, which is developing drone technology with California-based DreamHammer, [26] and STAR, which manufactures several trademarked network interception products.[27] The importation of military and police goods manufactured abroad is exempt from taxes and surveillance equipment is imported directly by the contracting agencies, although the contractor is held legally liable for the integrity of the goods. [28]

25 "Importador de inteligencia", El Espectador, 27 May 2011, http://www.elespectador.com/noticias/wikileaks/importador-de-inteligencia-articulo-259259

26 "DreamHammer Signs Drone Software Distribution Deal to Service Colombian Government Through Partner, Emerging Technologies Corporation", Business Wire, 15 May 2014, http://www.businesswire.com/news/home/20140515006450/en/DreamHammer-Signs-Drone-Software-Distribution-Deal-Service#.VM9YFId3aT8

27 "STAR Inteligencia & Tecnología", STAR Inteligencia & Tecnología, 2015, https://web.archive.org/web/20141225142051/http://www.star-it.co/

28 "Adquisición de Sistemas para el Fortalecimiento Tecnológico de la Plataforma Única de Monitoreo y Análisis (PUMA)", Administration and Finance Directorate, Ministry of Defence, 26 November 2013.

Network Surveillance

Network interception technologies are tools that require physical installation onto a network to perform communications surveillance. These tools are the modern more sophisticated and powerful versions of the crocodile clips of years gone by. Network interception technologies are contrasted with tactical technologies, which are mobile surveillance tools that do not require physical installation onto a network, but rather receive data either wirelessly or from devices directly.

The deployment of a network interception platform typically involves three types of commercial actors that provide different types of products and services. The first type of commercial actor is the manufacturer of the equipment that forms the basis of a network; examples include Nokia, Huawei and Alcatel-Lucent. The equipment such companies supply includes switches and exchanges used to connect traffic between lines, as well as other hardware and services which ensure telecommunications infrastructure, as a whole, is able to support different networks and services.

The second type of commercial actor is the telecommunications service provider (TSP) that manages a network and charges subscribers for services. TSPs are responsible for ensuring that their activities comply with the national legislation of the country where they operate. This usually includes statutory requirements that the TSP facilitate access by law enforcement and security agencies to their networks and to their subscribers' data. In Colombia, service providers are required to comply with interception requests from law enforcement agencies, pursuant to authorisation from the Fiscalía, according to Decree 1704 of the Ministry of Information Technology and Communications (MINTIC).[29] Article 44 of the 2013 Intelligence Law also mandates that telecommunications provided must comply with requests from intelligence and counterintelligence agencies to provide access to data and other technical assistance.

The third type of commercial actor is the surveillance technology company that directly markets and sells products and services for law enforcement purposes. These companies provide 'solutions' designed to enable state agencies to intercept, analyse, or disseminate data from networks. Surveillance companies sell these solutions either directly to governments or particular agencies or to TSPs in order to comply with the legal obligation in many countries that TSP's make their networks lawful interception compliant. Some TSPs therefore contract surveillance companies at their own expense, and incorporate electronic surveillance solutions within their networks.

29 Decree 1704 of 15 August 2012, Ministry of Information Technology and Communications, 15 August 2012, http://www.mintic.gov.co/portal/604/articles-3559_documento.pdf

Governments across the world including Colombia require that telecommunications providers make their networks compatible by applying and enforcing "Lawful Interception" standards. The Communications Assistance for Law Enforcement Act (CALEA) in the US and the European Telecommunications Standards Institute (ETSI) standards in Europe are two examples of legal frameworks designed to ensure that all telecommunications network equipment manufacturers and TSPs design telecommunication infrastructure to be accessible by states. Calls for bids for communications interception equipment in Colombia typically require that technology be to be CALEA-compliant.[30]

Colombia (2012)

Population (2013)	48,321,405 (World Bank)
Fixed Line Telephony Subscribers (2013)	7,141,461[31] (MINTIC)
Mobile Subscribers (2012)	49,066,359 (MINTIC)[32]
Fixed Internet Subcribers (2012)	4,047,032 (MINTIC)
Of which Broadband (2012)	3,918,266 (MINTIC)
Percentage of individuals using the Internet (2013):	51.7% (DANE)[33]

30 Asunto; Respuesta observaciones, Adquisición construcción y desarrollo tecnológico – Equipode Monitoreo de Telefonía Móvil Celular Nueva Tecnología – Sistema Integral de Grabación Digital – con Destino a la Policía Nacional", Police Revolving Fund, Ministry of Defence, 25 February 2005.

31 "Fixed Telephone Subsciptions (Excel)", International Telecommunication Union, http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

32 "Boletín trimestral de las TIC Cifras cuarto trimestre de 2012", MINTIC, March 2013, http://www.mintic.gov.co/images/documentos/cifras_del_sector/boletin_4t_banda_ancha_vive_digital_2012.pdf

33 "Percentage of Individuals using the Internet", International Telecommunication Union, http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

Mobile telephony service providers (2014) [34]

Total Subscriptions	51,594,619

Provider	Percentage of total subscriptions
Comcel	56.61%
Movistar	23.97%
Tigo	15.42%
Uff Móvil	0.79%
Une EPM	0.68%
Avantel	0.39%
ETB	0.09%
Virgin Mobile	1.66%
Éxito	0.38%

34 “Telefonía móvil: Participación en total de abonados por proveedor”, MINTIC, 2014, http://estrategiaticolombia.co/estadisticas/stats.php?&pres=content&jer=1&cod=&id=86#TTC

The companies: Network Surveillance

In this section we discuss the network interception technologies present in Colombia in the past five years and the foreign and domestic companies that provided them.[35]

STAR supplied technology for the Esperanza nationwide fixed-line and mobile interception platform using primarily their own technology, as well as products from US company Pen-Link and UK company Komcept Solutions.

Verint Systems Ltd built the Police's 'Integrated Recording System' using its own Vantage and Reliant interception solutions, provided and maintained by La Curacao. Verint Systems also built the Police's PUMA interception system. Another Israeli company NICE Systems in union with Colombian company Eagle Commercial won a number of later contracts to massively expand PUMA's interception capacity.

STAR Inteligencia & Tecnología and the Esperanza system

STAR registered as a company in May 2004 and for the following two years worked primarily on the Esperanza system.

STAR integrated components for the Esperanza interception system from British and American providers with its own equipment into a bespoke platform. Today, STAR provides interception hardware and software, big data analysis platforms and command and control centres among other security solutions, and is the sole authorised distributor of the products of a number of international companies. In addition, it is one of the few Colombian-owned companies that provides its own trademarked network interception equipment.

Komcept Solutions provided its Elucidate platform to STAR as part of Esperanza. Komcept Solutions has been selling lawful interception equipment to government customers from its rural Northamptonshire headquarters since 2001.[36] Among Komcept Solutions' portfolio of products is a mobile audio recording device resembling a briefcase that contains 144 digital microphones and a digital signal processor that can record from up to 30 metres away and relay data via Bluetooth to a remote analyst.[37] A Panama-registered company owned by STAR's executives, Expert Design Solutions, was responsible for maintaining the Komcept Solutions' equipment in Panama, the UK and the US.

35 This report is not a comprehensive list of companies present and/or selling surveillance technology in Colombia but an analysis of a number of the most significant surveillance technology suppliers and those integral to the network interception projects of the Colombian state. The companies profiled in this report sometimes sell both network interception and off-the-air interception technologies as part of their portfolio.

36 "Komcept Solutions Ltd." HM Government Companies House, 2015, http://data.companieshouse.gov.uk/doc/company/04291645



STAR COLOMBIA
Inteligencia & Tecnología

SALA SECCIONAL
Conectada con
PLATAFORMA CONTROL TELEMÁTICO

ITEM	DESCRIPCIÓN	CANTIDAD	VALOR UNIDAD	VALOR TOTAL
1	Sistema de Grabación ELUCIDATE-KOMCEPT: - Un (1) Sistema Elucidate: - 1 TB de almacenamiento. - Señal recibida desde sala Plataforma Control Telemático. - Equipos de interconexión. - Un (01) PRI o un (01) E1.	1	[redacted]	
	- Capacitación técnica y administrativa de los equipos que componen el sistema.		Incluida en el costo	

Sub TOTAL	$ [redacted]
IVA (16%)	$
TOTAL	$

NOTA: La Fiscalía General de la Nación debe suministrar un canal de comunicación entre la Plataforma de Control Telemático ubicada en el Búnker de la Fiscalía General de la Nación en Bogotá y la sala de monitoreo de la seccional a instalar, con el fin de realizar la transmisión de los datos y el audio enviados.

Validez de la Oferta: Un (01) mes.
Tiempo de Entrega: Tres (03) meses.
Precios: Los valores están dados en pesos colombianos.
Garantía: Los sistemas ofrecidos cuentan con una garantía de un (1) año contra defectos de fabricación. Se realizarán dos (02) visitas de mantenimiento preventivo. Se asignará un ingeniero como punto de contacto para requerimientos de soporte del sistema.

NOTA: Komcept (casa matriz) ha autorizado un descuento especial para la Fiscalía General de la Nación por un 50% de costo del equipo cotizado antes de impuestos. A continuación presentamos de nuevo la cotización con el descuento correspondiente.

Av El Dorado, # 68 C 61 Of 327 - 3 PBX (+57 1) 427 5077 FAX (+57 1) 427 5076 EMAIL star@star-colombia.com
www.star-colombia.com

DISCOUNT

Komcept Solutions provided special discounts to the Fiscalía to use its 'Elucidate' platform.

37 "DSEi 2009 Exhibition Show Preview", Defence Business, 2009, http://issuu.com/karlosullivan/docs/dbjuly

US technology firm Pen-Link provided the Esperanza interface that Colombian agents would use to manage and analyse intercepted phone data and content. Half of Pen-Link's business came from Latin America in 2010[38] and the company holds conferences in Bogotá to train law enforcement attendees from across the region to use its products.[39] Pen-Link also sells a server platform named Lincoln on which intercepted data is hosted. Lincoln can 'receive real-time intercept information delivered by the carriers, for any of the agency's legally authorised intercepts'. The collection process itself is controlled by the Pen-Link 8 client software.[40] Pen-Link is a preferred supplier of the US Drugs Enforcement Agency (DEA), engaging in over 170 contract actions with the agency since 1995, most in the past four years.[41] Pen-Link also supplied the US Embassy in Bogotá with 'target linkage software' which it regularly maintained over a period of years.[42]

Throughout the period of executing the Esperanza contract, STAR maintained very close ties with the Fiscalía. In 2009, a new Projects Director joined the company from the Fiscalia, whre he previously managed the telecommunications network of the Esperanza system and links to Colombian mobile providers' networks and reported to the Fiscalía's head of the Esperanza system, Vladimir Flórez Beltrán. STAR invited Beltrán to lunch meetings in 2008. STAR also covered the costs of tickets, hotel and associated travel costs in 2011 for another Fiscalía official to travel to the UK to verify two surveillance vehicles it contracted to buy from British firm LMW Electronics in 2011. Furthermore, STAR sought to open a joint back account with the Fiscalía in 2010, according to correspondence contained in the annex to this report.

Its proximity to the Fiscalía and central role in setting up Colombia's best known interception system afforded STAR very good connections within defence contracting circles. STAR had contact with all the main branches of the military and police services and the British, American and Mexican embassies. Business trips took STAR's director, Oscar Reyes, and Commercial Director and Projects Director to London, Los Angeles and New York to acquire and finalise contracts with providers. Other engineering employees travelled extensively throughout Colombia

38 "Mike Murman shares field notes from growing businesses", Nebraska Entrepreneurship, 15 December 2010, http://www.nebraskaentrepreneurship.com/news/mike-murman-shares-field-notes-from-growing-businesses/

39 "2012 Pen-Link Latin American Technical Training", Pen-Link, 15 March 2012 http://www.penlink.com/News/tabid/96/Default.aspx

40 "Lincoln Collection Systems", Pen-Link, 2015, http://www.penlink.com/Products/tabid/54/Default.aspx

41 "Contract Actions: Vendor Name: Pen-Link, Ltd., Department Full Name: Department of Justice," US General Services Administration, 20 April 2015, https://www.fpds.gov/ezsearch/fpdsportal?s=FPDSNG.COM&q=pen-link+VENDOR_FULL_NAME%3A%22PEN-LINK%2C+LTD.%22+CONTRACTING_AGENCY_NAME%3A%22DRUG+ENFORCEMENT+ADMINISTRATION%22&indexName=awardfull&y=0&templateName=1.4.4&x=0&STARt=0x

42 "Contract Actions: Vendor Name: Pen-Link, Ltd., Department Full Name: Department of State," US General Services Administration, 20 April 2015, https://www.fpds.gov/ezsearch/fpdsportal?indexName=awardfull&templateName=1.4.4&s=FPDSNG.COM&q=PEN-LINK+DEPARTMENT_FULL_NAME%3A%22STATE%2C+DEPARTMENT+OF%22+CONTRACTING_OFFICE_NAME%3A%22AMERICAN+EMBASSY+-+BOGOTA+-+GSO%22&x=0&y=0

implementing STAR's contracted surveillance projects. Several STAR engineers took turns attending to faults in the DAS' interception rooms throughout the weekends of 2009 and 2010.

The business model worked. STAR's sales increased ten-fold over its first five years, although it had only eleven employees in 2009. A true family business, at least three quarters of STAR's shares were held by Oscar Reyes' family in 2008.

Verint Systems, La Curacao and the Police platforms

Verint Systems Ltd, the Israeli sister company to US-headquartered Verint Systems Inc, sold mass surveillance technology to the Colombian police.

By the mid-2000s, the Police were calling for an expansion of their interception capabilities by pointing to the deficiencies of Esperanza. In particular, the police were concerned about Esperanza's interception quotas, technical dysfunctions and inability to deal with the increasing volume of internet protocol (IP)-based communications. The PUMA interception system was launched in 2007 as a 'monitoring' system administered and paid for by DIJIN.

PUMA is based on significantly more powerful and invasive technologies than Esperanza. It uses technology that is specifically designed to collect all data that passes through the cables for subsequent analysis. In this way it is 'passive', not requiring action from a Fiscalía agent to retrieve the information from a service provider. Rather, the system is linked directly to the service providers' network infrastructure, usually at the mobile switching centre (MSC), by a probe that routes all data directly to the law enforcement monitoring facility without interfering with the transmission of the data between the sender and recipient.

While PUMA was being built, another Police directorate built an interception platform, the Integrated Recording System (IRS), using the same technology as PUMA. The IRS could monitor 'massive communications traffic' across E1 lines and also 3G mobile phone traffic. It was not limited to targeted surveillance as documentation explains how it was capable of generating new targets.[43]

The Israeli wing of Verint Systems provided the technology on which the Police built both PUMA and the IRS. US-based Verint Systems Inc. is a software and hardware manufacturer specialising in data analytics and intelligence solutions while Israel-based Verint Systems Ltd. is responsible for communications surveillance products. Verint Systems was originally part of Comverse Technology, but in 2013 Verint acquired Comverse Technology's stake. Comverse Technology was founded in Israel by, among others,

43 "Respuesta observaciones: Contratación Directa No. 006 de 2005", Police Revolving Fund, Ministry of Defence, 25 February 2005.

Jacob 'Kobi' Alexander, who in 2006 was involved in a serious options backdating scandal.[44] As reported during the 2000s, Verint Systems was involved in supplying the wiretapping equipment to Verizon during the US National Security Agency warrantless wiretapping scandal.[45]

With 2014 revenues of US$ 910 million,[46] Verint Systems is among the few global leaders in monitoring centre technology. As part of its 'Communications & Cyber Intelligence' selection, it sells cyber security solutions, mobile tracking technology, tactical interception devices used to intercept mobile calls and open source analytical tools. For example, its SkyLock system claims to be able to track the location of a mobile phone anywhere in the world.[47] Targeted at TSPs and law enforcement and intelligence agencies, Verint Systems sells monitoring centres that 'enable the interception, monitoring, and analysis of target and mass communications over virtually any network' which, according to the company website, are in use in more than 75 countries.[48]

Verint Systems is known for supplying surveillance technology to governments who conduct widespread communications surveillance and political repression such as Kazakhstan and Uzbekistan, where activists, journalists, lawyers and politicians perceived to be opposed to the government are tightly monitored, as previously revealed by Privacy International.[49]

The company describes its monitoring centres as being split into two functional areas: a 'back-end', consisting of the monitoring centre itself where analysts request and receive data, and a 'front-end' located within the telecommunications network, which intercepts the data before sending it on to the monitoring centre.[50] When a request for data is made at the monitoring centre, the appropriate front-ends of the system located within the network

44 "In a Faded Wall St. Scandal, Lessons for a Current One", Solomon, S, 26 March 2013, http://dealbook.nytimes.com/2013/03/26/in-a-faded-wall-st-scandal-lessons-for-a-current-one/?_r=040

45 Bamford, James, "The Shadow Factory: The Ultra-Secret NSA from 9/11 to the Eavesdropping on America", 2008, Knopf Doubleday Publishing Group.

46 "Verint Announces Fourth Quarter and Full Year Results" Verint, 31 March 2014, http://www.verint.com/assets/verint/documents/january-31-2014-earnings-press-release-exhibit-99%201_3_31_14.pdf?_ga=1.84395997.57461801.1410275227

47 "For sale: Systems that can secretly track where cellphone users go around the globe" Timberg, Craig, The Washington Post, August 2014, http://www.washingtonpost.com/business/technology/for-sale-systems-that-can-secretly-track-where-cellphone-users-go-around-the-globe/2014/08/24/f0700e8a-f003-11e3-bf76-447a5df6411f_story.html

48 "Verint to supply new Swiss spying system", Swiss Info, 15 January 2014, http://www.swissinfo.ch/eng/verint-to-supply-new-swiss-spying-system/37740006

49 "Private Interests: Monitoring Central Asia", Privacy International, November 2014, https://privacyinternational.org/node/293

50 "Verint Selected To Provide Law Enforcement Communications Interception Solution To A New Customer in Asia Pacific", Verint, July 2002, http://phx.corporate-ir.net/phoenix.zhtml?c=131043&p=irol-newsArticle_print&ID=312250&highlight=

respond by intercepting the data and forwarding it on to the back-end.

Since 2005, the company has been central to the development of mass interception capabilities in Colombia, facilitated by their local representative and exclusive supplier La Curacao. Verint Systems engineers were responsible for the initial configuration of the system, while La Curacao engineers were responsible for preventative and corrective maintenance and training Police agents on its use.[51]

Through La Curacao, Verint Systems also supplied a network probe to the DAS sometime before 2011. As late as August 2011, while the DAS was being investigated for illegal interceptions (two months before it was formally dissolved), the DAS paid for La Curacao to 'ensure the full functioning and integrity of the internet information analysis system RELIANT by Verint Systems'.[52] This included maintaining the 'tactical probe' in whatever location in the country where it is operating, suggesting that it was a probe that could be removed and reinserted to tap cables as necessary. The US Embassy in Bogotá also contracted the US branch of Verint Systems for 'maintenance and support' of its intercept room.[53]

NICE Systems, Eagle Commercial and the PUMA expansion

In 2013, Colombian police sought to expand PUMA's interception capacity. Israeli technology company NICE Systems, in union with Colombian company Eagle Commercial was awarded a US$ 26 million (COP$ 50 billion) contract to expand the platform.

51 See for example, "Contrato de Prestación de Servicios PN-DIRAF N°__06-7-10124- 10", Directorate of Administration and Finance, Colombia National Police,1 September 2010, http://www.contratos.gov.co/consultas/detalleProceso.do?numConstancia=10-12-378033

"Contrato de Compraventa Celebrado entre la Dirección de Investigación Criminal y la Firma Compañía Comercial Curacao de Colombia S.A.", Directorate of Administration and Finance, Colombia National Police,April 2008, https://www.contratos.gov.co/archivospuc1/C/116001000/07-2- 88996/C_PROCESO_07-2-88996_116001000_446982.pdf (archived)

"Contrato de Prestación de Servicios PN-DIRAF N°__06-7-10120- 11", Directorate of Administration and Finance, Colombia National Police, 31 August 2011, http://www.contratos.gov.co/consultas/detalleProceso.do?numConstancia=11-12-598677

52 "Contrato de Prestación de Servicios de 2011, Celebrado entre el Fondo Rotario del Departamento Administrativo de Seguridad DAS Y Compañía Comercial Curacao de Colombia S.A.", Administrative Security Department Revolving Fund, 22 August 2011, http://www.contratos.gov.co/consultas/detalleProceso.do?numConstancia=11-12-620217

53 "List Of Contract Actions Matching Your Criteria: Verint, State Department, American Embassy Bogota", Federal Procurement Data System, 20 April 2015, https://www.fpds.gov/ezsearch/fpdsportal?s=FPDSNG.COM&q=VERINT+DEPARTMENT_FULL_NAME%3A%22STATE%2C+DEPARTMENT+OF%22+CONTRACTING_OFFICE_NAME%3A%22AMERICAN+EMBASSY+-+BOGOTA+-+GSO%22&indexName=awardfull&y=0&templateName=1.4.4&x=0

The expansion of PUMA would have provided the police with the ability to intercept 20,000 'objects' with the possibility of scaling up to 100,000. 'Super-PUMA' also flaunted new capacities, like a monitoring module for ISP traffic and up to 700 workstations throughout the country.[54] Data would be intercepted by way of eight 'NiceTrack IP' probes that 'filter and extract huge quantities of data delivered simultaneously over highly loaded IP links.'[55] For the first time in the history of Colombia's known interception systems, the system would be able to intercept 4G data.

Originally a manufacturer of surveillance products for military users only, NICE Systems today positions itself as 'the worldwide leader of intent-based solutions that capture and analyse interactions and transactions, realise intent, and extract and leverage insights to deliver impact in real time.'[56] Founded by seven former members of the Israeli Army,[57] it is based in Israel, although its shares are also traded on the US NASDAQ.

NICE Systems has three main branches. NICE Enterprise focuses on call centres and associated products including big data analytics and voice analysis. NICE Actimize focuses on analytical solutions for financial institutions to meet financial compliance requirements including anti-money laundering standards. NICE Security offers video-based surveillance solutions and associated analytics, as well as electronic surveillance technologies including tools for the interception of satellite phones. The NICE Systems monitoring centres on offer include capabilities to intercept, on a mass scale, telephone, mobile and IP data, and a location tracking centre that allows users to '[l]ocate anyone, anytime, anywhere' via mobile phones.[58] NICE Systems also markets various other analytical components that can be used in a monitoring centre, such as a Pattern Analyzer which aims to 'identify behavior irregularities that may point to criminal or terrorist activities.'[59]

Along with Verint Systems, NICE Systems is known for supplying surveillance technology to governments who conduct widespread communications surveillance and political repression such as Kazakhstan and Uzbekistan, where activists, journalists, lawyers and politicians perceived to be opposed to the government are tightly monitored, as revealed by Privacy International.[60]

54 "Asunto: Respuesta proposición N.04 de 2013", National Police of Colombia, 12 August 2013.

55 "NiceTrack™ Passive Interception for Packet Data and VoIP Networks", NICE Systems, 2007, http://www.nice.com/ru/files/IP_2007.pdf

56 "Company Overview", NICE Systems, 2015, https://web.archive.org/web/20150317125410/http://www.nice.com/company-overview

57 "NICE News Special Edition, vol. 2 iss. 3", NICE Systems, March 2006, https://web.archive.org/web/20131111045538/http://www.nice.com/news/newsletter/6_03s/anniversary.php

58 "Location Tracking", NICE Systems, 2015, https://web.archive.org/web/20150418214133/http://www.nice.com/intelligence-lea/location-tracking

59 "Pattern Analyzer", NICE Systems, 2015, https://web.archive.org/web/20150418203846/http://www.nice.com/intelligence-lea/pattern-analyzer

60 Private Interests: Monitoring Central Asia", Privacy International, November 2014, https://privacyinternational.org/node/293

NICE Systems lists some 25,000 organisations in more than 150 countries as customers and reported revenues in 2013 totalled US$ 951 million.[61] In May 2015, Israeli defence technology company Elbit Systems Limited signed an agreement to acquire NICE System's cyber and intelligence division.[62]

NICE System's Colombian partner in 2014 was Eagle Commercial SA. Eagle Commercial conducts business with the DAS, Police, Armed Forces and US Embassy among other clients. It also represents a number of international clients, including American Harris Corporation in 2006, and had acquired distributor relationships with Taser International Inc., maker of the electronic stunning equipment.[63] In 2010, it reported a profit of more than US$ 470 million after tax.[64]

Rival Interests

In the lawful interception market, Verint Systems and Nice Systems are considered rivals,[65] despite rumours in early 2013 that Nice Systems was in negotiations to acquire Verint Systems.[66] Their respective Colombian partners, La Curacao and Eagle Commercial are also rivals who have bid against each other for surveillance contracts.[67]

La Curacao fought hard to have an exclusive contract to maintain the PUMA system. In fact, the especially lucrative PUMA expansion contract turned into a better legal battle between the two gians and their Colombia proxies. La Curacao enjoyed at least COP$ 5 billion (US$ 2 million dollars) worth of exclusive contracts under the 'direct contracting' (contratación directo) process. This means that the contracting body (the Police, in this case) would select a

61 "NICE Reports Record Revenues and EPS for the Fourth Quarter and Full Year 2013", NICE Systems, 5 February 2014, https://web.archive.org/web/20150419014544/http://www.nice.com/nice-reports-record-revenues-and-eps-fourth-quarter-and-full-year-2013

62 "Elbit Systems Signs an Agreement to Acquire NICE Systems Cyber and Intelligence Division for an Amount of Up to $157.9 Million", Elbit Systems Limited, 21 May 2015, http://ir.elbitsystems.com/phoenix.zhtml?c=61849&p=irol-newsArticle&ID=2052104

63 "Importador de inteligencia", El Espectador, 27 March 2011, http://www.elespectador.com/noticias/wikileaks/importador-de-inteligencia-articulo-259259

64 "Importador de inteligencia", El Espectador, 27 March 2011, http://www.elespectador.com/noticias/wikileaks/importador-de-inteligencia-articulo-259259

65 "Verint Watches You, Should You Watch It?", Investopedia, 5 September 2012, http://www.investopedia.com/stock-analysis/2012/verint-watches-you-should-you-watch-it-vrnt-cmvt-nice-hpq0910.aspx and "Verint overtakes Nice to snatch Witness in a surprise move", Haaretz, 13 February 2007, http://www.haaretz.com/print-edition/business/verint-overtakes-nice-to-snatch-witness-in-a-surprise-move-1.212838

66 "Nice Systems in talks to buy Verint-report", Reuters, 14 January 2013, http://www.reuters.com/article/2013/01/14/nicesystems-verint-idUSL6N0AJ5GV20130114

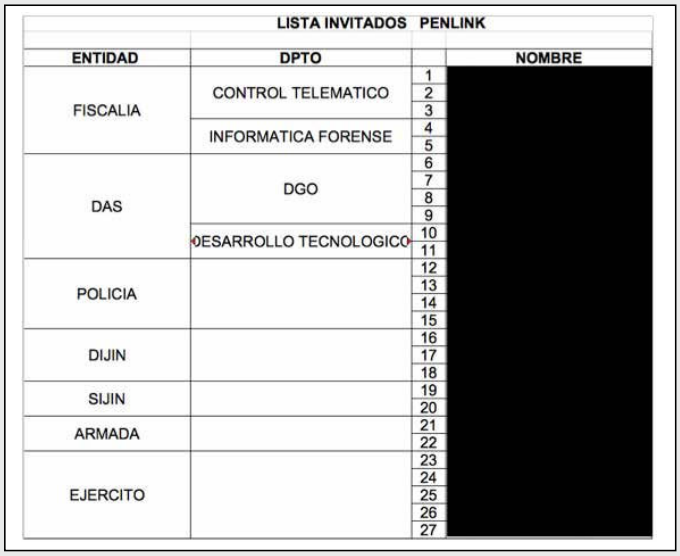
67 "Acta No.070 2006: Adjudicación de la Contratación Directa No. 057 de 2006", Police Rotating Fund, Ministry of Defence, 3 November 2006.

contractor without publishing a public call for bids (*convocatoria pública*).[68] But when, in 2010, La Curacao wrote to the Police arguing that La Curacao should have a direct contract lest 'untrained persons' without knowledge of the 'highly sophisticated and complex' Verint Systems system cause further damage to it, the Police answered that it was under no obligation to contract exclusively with the company.[69]

When NICE-Eagle obtained the PUMA expansion contract in November 2013, La Curacao and Verint struck back. In a January 2014 letter to the Transparency Secretary, Verint's attorney[70] submitted evidence alleging that NICE Systems had falsified engineer qualifications. Several months later, La Curacao was accused in a complaint to the office of the Comptroller General of having bribed Colonel Jairo Gordillo Rojas, former head of the police telematics unit, during the PUMA contracting process, including paying for all-expenses business trips to Europe.[71] Gordillo himself was questioned earlier that year over the illegal interception of journalists' phone calls.[72]

TAPS EVERYWHERE.

(Over)



LISTA INVITADOS PENLINK

ENTIDAD	DPTO		NOMBRE
FISCALIA	CONTROL TELEMATICO	1	[redacted]
		2	
		3	
	INFORMATICA FORENSE	4	
		5	
DAS	DGO	6	
		7	
		8	
		9	
	DESARROLLO TECNOLOGICO	10	
		11	
POLICIA		12	
		13	
		14	
		15	
DIJIN		16	
		17	
		18	
SIJIN		19	
		20	
ARMADA		21	
		22	
EJERCITO		23	
		24	
		25	
		26	
		27	

68 "Infografía: La Contratación Directa en Colombia", Kontrato.co, 5 August 2013, http://blog.kontrato.co/blog/2013/08/05/infografia-la-contratacion-directa-en-colombia/

69 "Asunto: Respuesta Observaciones: Actualización y Mantenimiento Plataforma PUMA", Police Administration and Finance Directorate, 30 March 2010, http://www.contratos.gov.co/archivospuc1/2010/ACL/116001000/10-9-120274/ACL_PROCESO_10-9-120274_116001000_1656021.pdf (archived)

70 "Contratos por más de US 35 millones para renovar salas de interceptación", Caracol Radio 2 5 April 2014, http://www.caracol.com.co/noticias/judiciales/contratos-por-mas-de-us-35-millones-para-renovar-salas-de-interceptacion/20140425/nota/2194095.aspx

71 "Las denuncias de corrupción contra el general León Riaño y sus hermanos", La F.M., 21 March 2014, http://www.lafm.com.co/noticias/las-denuncias-de-corrupcion-157475#ixzz3XqkMcdLm

72 "Fiscalía realiza interrogatorios por supuestas 'chuzadas'", Noticias RCN, 9 May 2014, http://www.noticiasrcn.com/nacional-pais/fiscalia-realiza-interrogatorios-supuestas-chuzadas

TAPS EVERYWHERE.



Bogotá D.C., Julio 17 de 2009

Señor Teniente Coronel:
Luis Vargas Valencia
Dirección de Inteligencia Policial
Ciudad

En nombre de Pen-Link Ltd y nuestros asociados en Colombia – STAR Inteligencia & Tecnología, lo invitamos cordialmente a participar en nuestra Conferencia para Latino América, la cual se llevará a cabo los días 10- 11 y 12 de Agosto, en el Hotel Sheraton, ubicado en la Avenida el Dorado No. 69 C 80.

El propósito de la Conferencia es mostrar los avances que se han tenido en el Área de Interceptación Legal a nivel técnico y de métodos, con el objetivo de llevar a cabo procesos adecuados en búsqueda de garantizar la seguridad de los ciudadanos y del Estado. Su experiencia y conocimiento en ésta área son particularmente invaluables.

Esperamos poder contar con su presencia tanto en las sesiones generales como en una reunión privada donde se podrá discutir abiertamente la forma como Pen-Link puede apoyar efectivamente a las agencias responsables para realizar Interceptación legal. Conscientes de sus múltiples ocupaciones y con el propósito de ajustar el horario de la reunión privada, le solicitamos nos informe la hora que más se ajusta a su agenda a fin de atenderlo como bien se merece, le agradecemos si esta verificación la realiza por intermedio de STAR Inteligencia & Tecnología.

Cordialmente,

OSCAR ALIRIO REYES CASTRO
Gerente General
STAR I&T S.A.

Av El Dorado No 68C 61 Oficina 327-3 www.star-colombia.com e-mail: star@star-colombia.com
PBX: +57 (1) 427 5077 Nit 830.139.912-1 FAX: +57 (1) 427 5076

STAR invited the DAS, Police (DIPOL and DIJIN), Navy (Armada), and Army officials as 'agencies responsible for conducting lawful interception' in addition to the Fiscalía to a promotional event at the Sheraton hotel in 2009. Pen-Link held an event complete with promotional clothing for representatives of agencies including the DAS, DIPOL and the Army's CITEC who were invited to witness demonstration's of Pen-Link's products and progress that has been made in the area of legal interception'.

The decision to choose NICE Systems over Verint Systems was in all likelihood due to rivalries between defence contractors trying to pitch their products to a government ever more eager to prove results, with the PUMA contract being a particularly lucrative one, according to individuals close to the process.[73] Whatever the reason, the concern over potential corruption obscured discussion in the media about just how powerful the new 'Super-PUMA' would be.

Other European Companies

Other companies have been marketing and selling products to Colombian authorities carrying out surveillance.

One example is UK headquartered technology firm Network Critical that provided fibre optic passive traffic access points (TAPs) to DIPOL, according to a delivery notice contained in the annex. It is not clear how they related, if at all, to DIPOL's existing surveillance program, the Integrated Recording System.

NetworkCritical produces 'network visibility controllers' and created the network TAP solution.[74] In the private sector, such technologies, also known as network 'sniffers',[75] can help enterprises detect data leaks and monitor how visitors are engaging with their sites. As these techniques analyse and monitor traffic, they are, by design, suitable for electronic surveillance, and are widely used for electronic surveillance and censorship across the world. The SlimLine TAP products offered to DIPOL are designed to enhance monitoring centre performance by allowing for access to live network traffic and by providing copies of data flow to separate monitoring ports in the centre.[76] SlimLine is compatible with a number of vendors' interception products, including Verint Systems.[77]

73 On 30 March 2010, DIJIN responded to La Curacao's complaint. The Directorate responded that they were not obligated to contract solely with La Curacao, citing the need for transparency in the selection process.

74 "Network Critical is the Preferred TAP Solution for Use with the Enterasys Intrusion Prevention System (IPS).", Network Critical, 15 September 2010 https://networkcritical.wordpress.com/2010/09/15/network-critical-is-the-preferred-tap-solution-for-use-with-the-enterasys-intrusion-prevention-system-ips/

75 Network Critical" Sourcefire, 2015, http://www.sourcefire.com/partners/technology-partners/sourcefire-technology-partners/network-critical

76 "Passive Taps", Network Critical, 2015, http://www.networkcritical.com/products/passive-taps

77 "Lawful Interception Deployments", Network Critical, 2011, http://www.networkcritical.com/NetworkCritical/media/resource-library/other/Network-Critical-Solution-Deployment-Lawful-Interception.pdf

Tactical Surveillance

Tactical surveillance technologies are surveillance tools that collect intercepted communications data either wirelessly or directly from a target device rather than from the service provider's network architecture. Often they can be easily transported to different locations for deployment. Technologies such as IMSI catchers[78] and intrusion tools[79] are all present in Colombia and are used by different government agencies.

The companies: Tactical surveillance

Many international and national companies provided tactical interception products to Colombian law enforcement and intelligence agencies. Vendors that have competed to sell interception products to the Police and the DAS include New Zealand-headquartered Spectra Group and UK-based Smith Myers. DAS agents used software from US company AccessData in mobile forensic units that could be used to obtain private data directly from target devices. Finally, the Police has conducted business with Hacking Team, a technology company headquartered in Italy best known for producing offensive malware that essentially allows for hacking and remote control of target devices.

One of the most common tactical interception products is an IMSI catcher, commonly known as 'stingrays' in the US.[80] Two unique numbers identify mobile devices: the International Mobile Subscriber Identity (IMSI), which identifies a caller's SIM card, and the International Mobile Station Equipment Identity (IMEI), which identifies the actual device. Both numbers are routinely communicated to network providers as the user moves about. Certain location monitoring technologies identify activity corresponding to these two numbers that the monitoring body may see as suspicious, such as SIM card swapping (the IMEI number would remain the same but the IMSI number changes frequently).

IMSI catchers are monitoring devices that transmit a strong wireless signal that entices nearby phones to connect to it and transmit communications data and content; they can be retrofitted with location monitoring technologies that determine the location of a target to within one metre. These devices could be 'targeted' towards a particular individual's device by, for example, being aimed at his or

78 "Phone Monitoring", Privacy International, 2015, https://privacyinternational.org/?q=node/76

79 "Intrusion", Privacy International, 2015, https://privacyinternational.org/?q=node/73

80 "Florida Cops' Secret Weapon: Warrantless Cellphone Tracking", Wired, 3 March 2014, http://www.wired.com/2014/03/stingray/

her workplace, but they can also be used to identify unknown persons attending demonstrations and other gatherings because as many mobile phones as the system can accommodate will connect to the IMSI catcher.

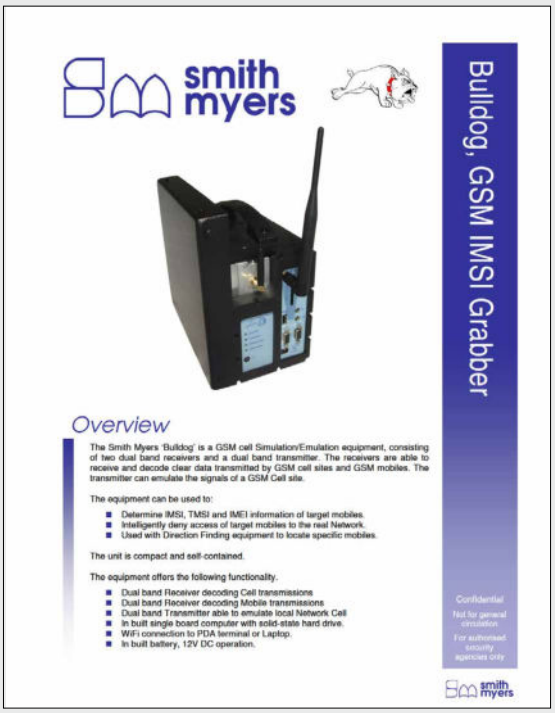
Many companies offer IMSI catchers in Colombia. New Zealand-based Spectra Group via Colombian company Maicrotel Ltda provided its Laguna IMSI catcher to DIPOL in September 2005. The Laguna system is designed to monitor and record telephone conversations and data in mobile communication systems and could be mobile or assembled in fixed stations.[81] Bulldog and Nesie, manufactured by UK surveillance company Smith Myers, are two other popular IMSI catchers sold in Colombia. In 2010, the DAS was preparing to purchase a Bulldog interception system for over US$ 250,000 and a Nesie system for over US$ 320,000. The Fiscalía was also planning to buy a Bulldog system for just over US$ 280,000 as was the sectional division of DIJIN in Bogotá. In 2014, the Finnish branch of Canadian telecommunications company Exfo exported its NetHawk F10 IMSI catcher to Colombia.

81 "Contrato de Compraventa No. 152 de 2005, celebrado entre el Fondo Rotatorio de la Policía y la Firma M@icrotel LTDA.", Police Revolving Fund, 30 September 2005.



Bidders for one 2006 contract had to demonstrate the capacities of their products by intercepting targets' phones in select Bogotá locations including Centro Comercial Portal Calle 80, pictured here.[82] Credit: Privacy International (2014)

82 "Adjudicación de la Contratación Directa No. 055 de 2006", Police Revolving Fund, Ministry of Defence, 29 November 2006, https://www.contratos.gov.co/archivospuc1/ADA/115001003/06-2-16355/ADA_PROCESO_06-2-16355_115001003_31717.pdf (archived)





POPULAR ITEMS

UK firm Smith Myers' product, Bulldog simulates mobile phone base station sites to connect with mobiles in a target area and to retrieve their identifying information (IMSI, TMSI and IMEI). Bulldog is supposed to, with direction finding equipment, locate target devices and their users from among a pool of devices in a given area. Nesie, another Smith Myers product, also elicits the identifying information of mobile phones in the area by simulating mobile base station sites. It can deny access of specific phones to the real network, forcing those phones to connect with the Nesie device and communicate real-time unencrypted call content to Nesie operators.

A person's communications can also be obtained physically from their device. For example, an agent could forensically copy the communications data contained in a device seized covertly or at point of arrest. In July 2007, the DAS published technical specifications for a tender for equipment that would allow them to copy and inspect targets' devices. Although the bid was ultimately cancelled in December 2006, the DAS acquired the technology before 2010. La Curacao won a maintenance contract, beating out competitors Internet Solutions Ltda and SF International. The software the DAS used was Forensic Toolkit (FTK), a computer forensics software made by US-based AccessData. The 3.0 FTK software specified in the 2010 contract allows the analyst to not only 'preview a target's machine from across the network to determine relevancy prior to acquisition, but ... also acquire and fully analyse the data on the system,

including the system's RAM [random access memory]'.[83] A remote drive feature enables analysts to forensically analyse live data – such as system memory, logical volumes, physical devices – on a remote device from the analyst system. The software could also be used to decrypt PGP-encrypted disks.[84]

Offensive malware is a particularly invasive surveillance tool that is used to target a known device. It can attack a target by encouraging the target to allow the software to install itself, for example, by way of false security updates or apparently innocuous downloads. Once installed the malware attacks and exploits the device's memory and operating system, allowing an analyst to remotely control the device. Intrusion software or malware is generally marketed as filling a perceived gap between passive interception (such as network monitoring) and physical searches, by allowing a third party direct access to data stored, sent and received on an infected target device. Such equipment can be integrated into the monitoring centres of specific agencies and used directly by law enforcement and intelligence agencies. The companies manufacturing these types of technologies regularly exhibit their products at surveillance and security trade shows. Use of intrusion technologies is unlawful and not accounted for under Colombian law.[85]

Hacking Team produces an intrusion system that was acquired by the Colombian police. The company's Remote Control System (RCS) can be used to hijack computer and mobile devices while remaining undetectable to users, as it is designed to bypass common antivirus programmes and encryption. By infecting a target's device, the RCS suite can capture data on a target's device, remotely switch on and off webcams and microphones, copy files and typed passwords. In 2014, Hacking Team had a Colombia-based field engineer and an active contract with the Colombian police. The Colombian government's use of offensive Hacking Team malware products had been suspected since researchers at the Citizen Lab identified a command and control server for the RCS suite in Colombia.[86] Hacking Team supplied its technology to the DEA, which according to internal emails was reportedly using the spyware to conduct surveillance from the U.S. embassy in Bogotá.[87] Hacking Team also had two projects with the Colombian police, one of which appears to relate to the PUMA surveillance system. [88]

83 "AccessData Releases Forensic Toolkit® 3.0", AccessData, 22 September 2009, https://ad-pdf.s3.amazonaws.com/FTK3_press_release.pdf

84 The decryption would be accomplished by obtaining the decryption keys from the device, not by actually breaking the encryption key itself. "AccessData FTK 3.0.4 Release Notes", AccessData, 2009, https://ad-pdf.s3.amazonaws.com/ftk3-0-4readme.pdf

85 Nevertheless Colombian company, Emerging Technologies Corporation reports selling 'remote intrusion solutions for PCs'. "Inteligencia de Señales", Emerging Technologies Corporation, 2015, http://etcsa.com/sistemas-de-informacion-e-inteligencia/inteligencia-de-senales/

86 "Mapping Hacking Team's 'Untraceable' Spyware", The Citizen Lab, 17 February 2014, https://citizenlab.org/2014/02/mapping-hacking-teams-untraceable-spyware/

87 "Hacking Team emails expose proposed death squad deal, secret U.K. Sales push and much more", The Intercept, 9 July 2015, https://firstlook.org/theintercept/2015/07/08/hacking-team-emails-exposed-death-squad-uk-spying/

88 "El software espía de la Policía", El Espectador, 11 July 2015, http://www.elespectador.com/noticias/investigacion/el-software-espia-de-policia-articulo-571980

Conclusion

The surveillance industry is the lifeblood of state surveillance activities worldwide. Companies such as Verint Systems, NICE Systems, Pen-Link, Komcept, Hacking Team and their Colombian partners including STAR, Eagle Commercial and La Curacao facilitate state surveillance. They thus bear a degree of responsibility for their activities' lawfulness and the impact they are having on human rights.

Companies providing mass surveillance systems directly enable disproportionate, indiscriminate surveillance in contravention of internationally established human rights principles.

No more than a handful of individuals within the industry appear to have adequately considered the human rights impacts of their businesses. This is despite extensive evidence that the industry is having an adverse impact on the enjoyment of human rights across the world.

Rather than recognise their own responsibilities, companies tend to deflect blame and responsibility for misuse of surveillance technologies by focusing on the responsibilities of the end-user ofthe products and services they supply. The focus runs contrary to established principles governing the corporate responsibility to respect human rights. The fact that a state violates human rights does not lessen the responsibilties of a company to respect human rights. In circumstances in which sales of technology could result in human rights abuses, those responsiblities are also increased.

Greater transparency is undoubtedly a prerequisite to understanding the surveillance industry's impact on human rights. With limited information, it is exceptionally difficult for civil society organisations to hold surveillance companies to account for human rights abuses. The onus is on the companies not only to be more transparent, but also to properly understand their human rights impacts and take action to prevent human rights abuses resulting from the use of the products and services they provide to states.

The chief means by which companies can limit the deletrious effects of the use of their products and services on human rights is by ensuring that they are not actively involved in the development of other countries' surveillance capabilities if they are being used in connection with interferences with human rights, democratic principles or freedom of speech. Furthermore, states should adopt export controls on the sale of surveillance technologies to law enforcement and intelligence agencies in countries with poor human rights records. Those controls should be informed by strong human rights based criteria to ensure that companies within their jurisdiction do not export to end-users where there is a risk the transfer poses a threat to human rights.

Annex 1: Quote for sale of Smith Smyers' Bulldog product to DAS

XXXXXXXXXXX

	FORMATO DE COTIZACIÓN STAR INTELIGENCIA & TECNOLOGÍA	VERSION :1 CODIGO: GC-FO-47 FECHA DE APROBACION: 28 DE MAYO 2010

Señores:	DEPARTAMENTO ADMINISTRATIVO DE SEGURIDAD DAS
Contacto:	Ing. Ramiro Ordoñez
Dirección:	Carrera 27 # 17A - 00
Telefóno:	408 80 00 Ext. 2108
E-mail:	coordinacioncienciaytecnologia@das.gov.co
Ciudad:	Bogotá DC

GC-151-Cotización

ITEM	REF.	DESCRIPCION	CANT.	UND.	VR. UNITARIO	VALOR TOTAL
1	BLDG	**Kit analizador de espectro y sistema de goniometría para ingeniería de redes móviles. Incluye los siguientes componentes: receptor panorámico 824 - 894 MHz "Bulldog" (1); goniómetro móvil HHDF (1)**	1	UND.	[redacted]	
					SUBTOTAL	[redacted]
					IVA	
					TOTAL	

CONDICIONES COMERCIALES	
MONEDA DE LA OFERTA	Pesos Colombianos
VALIDEZ DE LA OFERTA	30 días
TIEMPO DE ENTREGA	A convenir
FORMA DE PAGO	50% de anticipo; 30% contra notificación de embarque; 20% contra entrega a satisfacción.
GARANTIA	12 meses
OBSERVACIONES	Estos bienes pueden estar exentos de IVA. Literal d) del estatuto tributario, concepto 06094 de 1999 y concepto unificado 003/2003 de la DIAN.

[redacted]

Annex 2: Letter related to opening of joint bank account between STAR and Fiscalia

XXXXXXXXXXX

Bogotá D.C. 25 de Noviembre de 2010

Señores
BANCOLOMBIA
Ciudad

GG-OF-402

Por medio de la presente autorizo al señor [redacted] identificado con Cédula de Ciudadanía No. [redacted] e Manizales, para recoger documentación de apertura de cuenta conjunta entre STAR Inteligencia & Tecnología S.A. y Fiscalía General de la Nación.

Gracias por su atención

Cordialmente

STAR Inteligencia & Tecnología S.A.

Oscar Alirio Reyes Castro
Representante Legal

Annex 3: Star offering to cover costs of Fiscalia official trip to the United Kingdom as per contract

XXXXXXXXXXX

Bogotá 02 de Febrero de 2011

Asistente No. 12

Señores
Embajada Británica
Ciudad

Respetados Señores:

Por medio de la presente notificamos que la señora [redacted], identificada con Cedula de Ciudadanía No. [redacted]e Bogotá, es funcionaria de la Fiscalía General de la Nación y está aplicando a la Visa del Reino Unido, como delegada de esta entidad del Gobierno, para una visita que se realizará a la Fabrica LMW Electronics. Esto con el propósito de realizar la verificación de funcionamiento de los equipos que serán despachados a Colombia bajo el contrato No. 093 de 2010, firmado entre la Fiscalía General de la Nación y STAR Inteligencia & Tecnología S.A.

Es de aclarar que los gastos por concepto de tiquetes, hotel y viáticos serán cubiertos por nuestra compañía, como quedó estipulado en clausulas del contrato mencionado.

Cordialmente,

Oscar Alirio Reyes Castro
Gerente General