The Surveillance Industry in India

By *Maria Xynou*

March 2014[1]

India has the world's second largest population, an expanding middle class and undoubtedly a huge market which attracts international investors. Some of the world's largest corporations have offices in India, such as Google Incorporated and BlackBerry Limited. In the Information Age, the market revolves around data and companies which produce technologies capable of mining such data are on the rise[2]. Simultaneously, companies selling surveillance technologies appear to be on the peak too, especially since the global War on Terror requires law enforcement agencies around the world to be equipped with the latest surveillance gear[3].

Terrorism is undoubtedly a major issue in India, especially in light of the numerous terrorist attacks over the last twenty-five years[4]. With a population of over a billion people and high levels of mass poverty, multiple religions, languages, and ethnicities - crime also appears to be a major security threat in India. As such, Indian law enforcement agencies are in need of tools to aid them in tackling crime and terrorism in the country. Such tools can include various types of surveillance technologies, which are being used by law enforcement agencies around the world[5].

The Centre for Internet and Society (CIS) has undertaken research to investigate the potential growth of the surveillance industry in India – especially in light of the Mumbai 2008 terrorist attacks[6]. Some of the biggest surveillance technology companies in the world, such as ZTE, Utimaco and Verint Systems, have offices in India. FinFisher command and control servers have been found in India[7]. In addition to foreign security companies based in India, local security companies appear to be on the rise too. This paper aims to share the CIS' research on India's potential for a surveillance industry, which is based on publicly available information.

Security Companies operating in India

[1] As a note: The research for this paper was undertaken in 2013 and thus the information in the paper reflects what was available at that time.

[2] Theresa Krause, *"Data Mining in the Information Age"*, University of Utah, November 2011, http://www.law.utah.edu/wp-content/uploads/Data-Mining-in-the-Information-Age-Krause.pdf

[3] Nick Hopkins & Matthew Taylor, *"Private firms selling mass surveillance systems around world, documents show"*, The Guardian, 18 November 2013, http://www.theguardian.com/world/2013/nov/18/private-firms-mass-surveillance-technologies

[4] Sabir Shah, *"Major terror attacks in India during last 25 years"*, The International News, 28 October 2013, http://www.thenews.com.pk/Todays-News-2-210676-Major-terror-attacks-in-India-during-last-25-years

[5] Nick Hopkins & Matthew Taylor, *"Private firms selling mass surveillance systems around world, documents show"*, The Guardian, 18 November 2013, http://www.theguardian.com/world/2013/nov/18/private-firms-mass-surveillance-technologies

[6] CNN Library, *"Mumbai Terror Attacks"*, 19 September 2013, http://edition.cnn.com/2013/09/18/world/asia/mumbai-terror-attacks/

[7] Morgan Marquis-Boire, Bill Marczak, Claudio Guarnieri & John Scott-Railton, *"For Their Eyes Only: The Commercialization of Digital Spying"*, The Citizen Lab, 30 April 2013, https://citizenlab.org/2013/04/for-their-eyes-only-2/

Research sample 1: 76 security companies in India

The Centre for Internet and Society (CIS) initiated its research on security companies by selecting a random sample of 100 companies based in India which belong to the security sector. Out of the 100 companies, 76 of these companies appeared to sell products which belong in one – or more – of the following categories[8]:

- Internet monitoring software
- Malware (trojans, spyware, etc.)
- Social network analysis software
- Data mining and profiling software
- Phone monitoring software
- SMS monitoring software
- Speech analysis/ Voice recognition software
- Surveillance of location
- GPS tracking equipment
- RFID
- Analytics
- Surveillance cameras (e.g. CCTV cameras)
- Aerial surveillance (drones)
- Biometric collection
- Access control systems

The reason why these companies were randomly selected was to reduce the probability of research bias and out of the 100 companies initially selected, 76 of them turned out to sell products from the above categories. It should be noted that most of these companies are not restricted to surveillance technologies, but also produce other non-surveillance technologies. Indeed some of these companies simultaneously produce Internet monitoring software and encryption tools[9].

The 76 companies selling products which fall in the above listed categories can be viewed in Table 1[10]. Some of these companies are Indian, whilst others have international headquarters and offices in India. Not surprisingly, the majority of these companies are based in India's IT hub, Bangalore. Table 2[11] shows the types of products sold by each of the 76 companies.

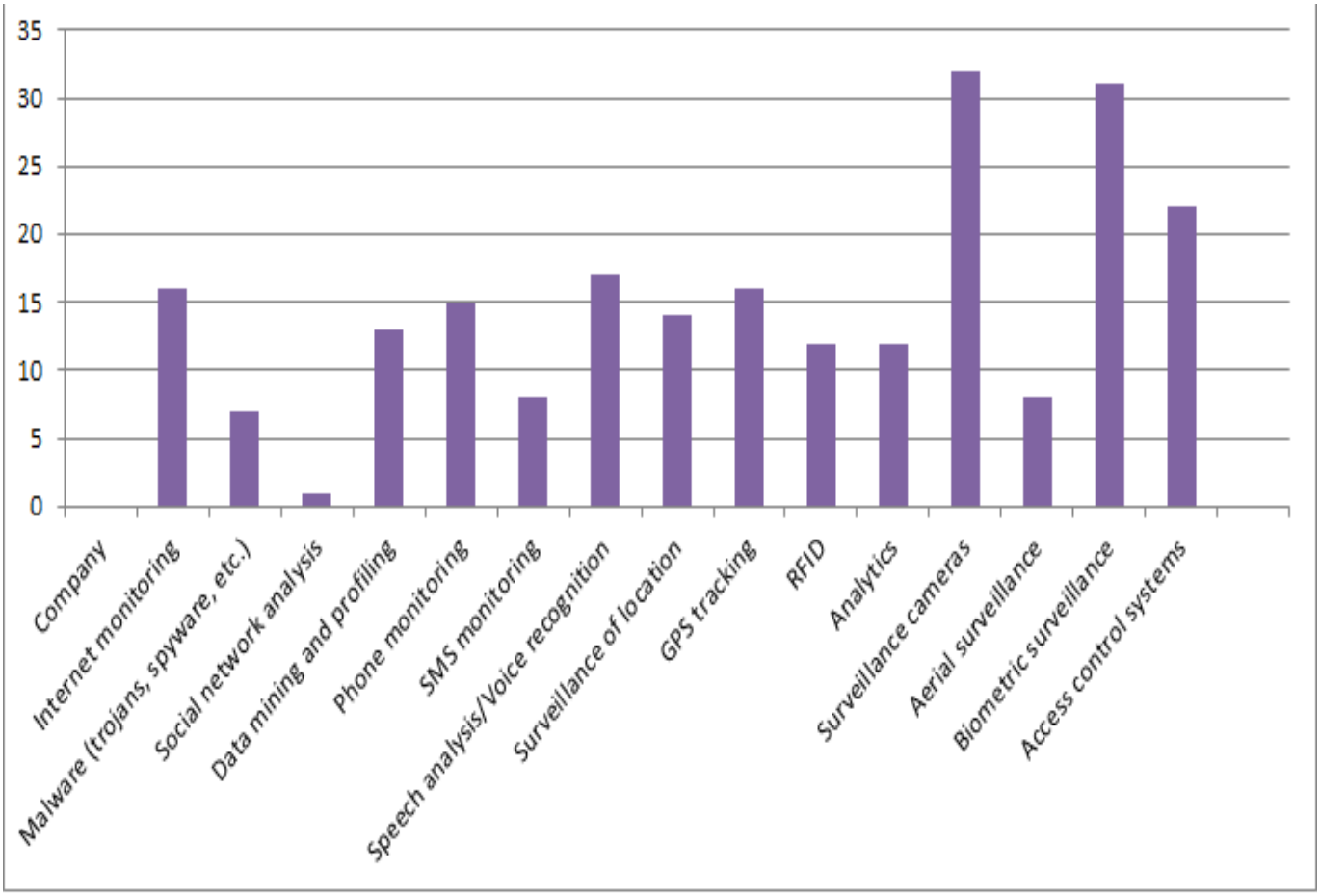
The graph below is based on Table 2 and shows which types of security solutions are produced the most by the 76 companies.

[8]Maria Xynou, *"The Surveillance Industry in India: At Least 76 Companies Aiding Our Watchers!"*, The Centre for Internet and Society, 02 May 2013, http://cis-india.org/internet-governance/blog/the-surveillance-industry-in-india-at-least-76-companies-aiding-our-watchers

[9]Ibid

[10]Centre for Internet and Society, *Surveillance Industry: Table 1*, 02 May 2013, http://cis-india.org/internet-governance/blog/table-1.pdf

[11]Centre for Internet and Society, *Surveillance Industry: Table 2*, 02 May 2013, http://cis-india.org/internet-governance/blog/table-2.pdf



Out of the 76 companies, the majority (32) sell surveillance cameras, whilst 31 companies sell biometric technology; this is not a surprise, given the UID scheme which is rapidly expanding across India. Only one company from the sample produces social network analysis software, but this is not to say that this type of technology is low in the Indian market, as this sample was randomly selected and many companies producing this type of software may have been excluded. Moreover, many companies (13) from the sample produce data mining and profiling technology, which could be used in social networking sites and which could have similar - if not the same - capabilities as social network analysis software[12]. In addition, the graph shows that 15 companies sell phone monitoring software, while 73% of the population in India uses mobile phones[13]. This could imply that there is possibly a high probability of high levels of mobile surveillance in the country.

Key facts about some of the companies within the sample include the following[14]:

- WSS Security Solutions Pvt. Ltd. is considered to be north India´s first CCTV zone
- Speck Systems Limited was the first Indian company to design, manufacture and fly a micro UAV indigenously
- Mobile Spy India (Retina-X Studios) has the following mobile spying features:

1. *SniperSpy*: remotely monitors smartphones and computers from any location

[12]Ibid
[13]We are Social, *India,* 2014 Edition, http://wearesocial.net/tag/india/
[14]Maria Xynou, *"The Surveillance Industry in India: At Least 76 Companies Aiding Our Watchers!",* The Centre for Internet and Society, 02 May 2013, http://cis-india.org/internet-governance/blog/the-surveillance-industry-in-india-at-least-76-companies-aiding-our-watchers

2. *Mobile Spy:* monitors up to three phones and uploads SMS data to a server using GPRS without leaving traces

- Infoserve India Private Limited produces an Internet monitoring System with the following features:

1. Intelligence gathering for an entire state or a region
2. Builds a chain of suspects from a single start point
3. Data loss of less than 2%
4. 2nd Generation Interception System
5. Advanced link analysis and pattern matching algorithms
6. Completely Automated System
7. Data Processing of up to 10 G/s
8. Automated alerts on the capture of suspicious data (usually based on keywords)

- ClearTrail Technologies deploys spyware into a target´s machine
- Spy Impex sells Coca Cola Tin Cameras
- Nice Deal also sells Coca Cola Spy Cameras, as well as Spy Pen Cameras, Wrist Watch Cameras and Lighter Video Cameras among other products
- Raviraj Technologies is an Indian company which supplies RFID and biometric technology to multiple countries all around the world. Countries served by Raviraj Technologies include non-democracies, such as Zimbabwe and Saudi Arabia, as well as post-revolutionary countries, such as Egypt and Tunisia[15].

Research sample 2: 50 security companies in India

This research was further limited to a random sample of 50 companies, which were subsequently analysed in more detail. The initial sample of 76 companies comprised of many re-seller companies, which sold products and solutions produced by other companies. The random sample of 76 companies was narrowed down to 50 companies with the aim of subtracting most re-seller companies from the sample and limiting it mainly to companies which sell products and solutions they produce.

Furthermore, additional fields of research were added when examining the sample of 50 companies. The new data illustrates the companies which were analysed and includes data with regards to their contact details, the type of security solutions they sell, their customers and their compliance (or non-compliance) with lawful regulations and certification standards[16]. In other words, this research was expanded to include the details of the types of solutions that these companies sell, the type of customers they sell them to, whether they include privacy policies on their websites and whether their solutions are certified and compliant with lawful regulations.

Out of the 50 companies from the random sample, 40 companies are headquartered in India, while the following 10 companies have international headquarters[17]:

1. Shield Security (UK)
2. Utimaco (Germany)
3. Fulcrum Biometrics (USA)

[15]Ibid
[16]Maria Xynou, *Spreadsheet data on sample of 50 security companies*, Centre for Internet and Society, 28 February 2014, http://cis-india.org/internet-governance/blog/data-on-surveillance-technology-companies
[17]Ibid

4. Iritech (USA)
5. Smartmatic (UK)
6. Mobile Spy (USA)
7. Verint Systems (USA)
8. Aqsacom (France)
9. Polaris Wireless (USA)
10. Polixel Security Systems (Poland)

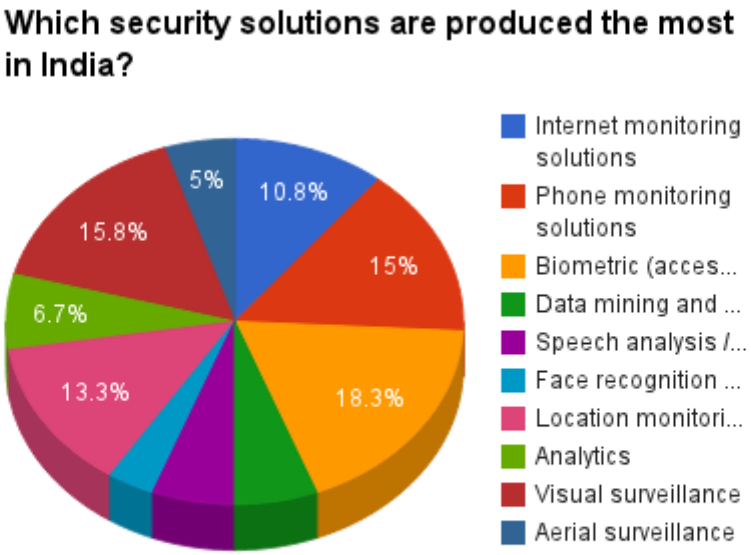
Security Solutions

All 50 companies from the sample produce and sell security solutions from one – or more – of the following categories[18]:

- Internet monitoring software
- Data mining and profiling software
- Phone monitoring software
- Speech analysis / Voice recognition software
- Face recognition software
- Location monitoring
- Analytics
- Visual surveillance
- Aerial surveillance
- Biometric (access control) systems

The following pie chart illustrates which security solutions are produced the most by the 50 security companies of the random sample:

[18] Ibid



The above pie chart is based on the data collected on each of the 50 companies, as illustrated in the new data[19]. In particular, it is evident that biometric technologies and access control systems are produced the most (18.3%), while surveillance cameras (15.8%) and phone monitoring software (15%) are also prevalent in the security industry. Internet monitoring solutions (10.8%) are also produced by the 50 companies of the sample, as are location monitoring solutions (13.3%), such as RFID and GPS tracking devices. While the above chart is not necessarily representative of the entire security industry in India, it could indicate that biometric technology, access control systems, Internet and phone monitoring solutions, as well as RFID and GPS tracking devices are high in demand.

Notable security companies

Kommlabs Dezign is an Indian company which sells its Internet monitoring solutions at various ISS trade shows[20]. In particular, Kommlabs Dezign sells VerbaNET, an Internet Interception Solution, as well as VerbaCENTRE, which is a Unified Monitoring Centre that can detect cognitive and emotional stress in voice calls and flag them. VerbaCENTRE also provides Central Monitoring Centres and Regional Monitoring Centres for countrywide deployment[21].

Vehere is another Indian company which sells various surveillance solutions and notably sells vCRIMES, which is a Call Details Records (CDR) analysis system. VCRIMES is used to analyse and gather intelligence and to unveil hidden interconnections and relations through communications. This system also includes a tool for detecting sleeper cells through advanced statistical analysis and can analyse more than 40 billion records in less than 3 seconds[22].

Paladion Networks is headquartered in Bangalore, India and sells various Internet Monitoring Systems, Telecom Operator Interception Systems, SSL Interception and Decryption Systems and Cyber Cafe Monitoring Systems. Paladion Networks states in its website that its customers include India's Ministry of Information Technology and the U.S Department of Justice. Furthermore, Paladion Networks supplies security solutions to its 700 customers in 30 countries across Asia, the

[19]Ibid
[20]Kommlabs Dezign, *Events*, http://www.kommlabs.com/events.asp
[21]Kommlabs Dezign, *Solutions for Intelligence Agencies*, http://www.kommlabs.com/solutions-intelligence.asp
[22]Vehere, *vCrimes*, http://www.veheretech.com/products/vcrimes/

U.S and Europe[23].

Verint Systems is headquartered in New York and has offices all around the world, including Bangalore in India. Verint Systems produces a wide range of surveillance technologies, including "Vantage" which intercepts, filters, and analyzes mass and target communications from traditional voice, Internet, mobile, fixed satellite, and cellular communications in compliance with lawful interception mandates. This monitoring center is designed to help intelligence, national security, and other government agencies to generate high-quality intelligence from huge volumes of data[24]. Furthermore, Verint's "STAR-GATE" solution is designed to manage vast numbers of targets, concurrent sessions and networks, and to transparently access target communications[25].

ClearTrail Technologies is an Indian company based in Indore. The document titled "Internet Monitoring Suite" from ClearTrail Technologies illustrates the company's mass monitoring, deep packet inspection, COMINT, SIGINT, tactical Internet monitoring, network recording and lawful interception technologies[26]. ClearTrail's Internet Monitoring Suite includes the following products:

1. ComTrail: Mass Monitoring of IP and Voice Networks

ComTrail is an integrated product suite for centralized interception and monitoring of voice and data networks. It is equipped with an advanced analysis engine for pro-active analysis of thousands of connections and is integrated with various tools, such as Link Analysis, Voice Recognition and Target Location[27].

ComTrail is deployed within a service provider network and its monitoring function correlates voice and data intercepts across diverse networks to provide a comprehensive intelligence picture. ComTrail supports the capture, record and replay of a variety of Voice and IP communications in pretty much any type of communication, including - but not limited to- Gmail, Yahoo, Hotmail, BlackBerry, ICQ and GSM voice calls[28].

Additionally, ComTrail intercepts data from any type of network -whether Wireless, packet data, Wire line or VoIP networks- and can decode hundreds of protocols and P2P applications, including HTTP, Instant Messengers, Web-mails, VoIP Calls and MMS.

In short, ComTrail's key features include the following[29]:

- Equipped to handle millions of communications per day intercepted over high speed STM & Ethernet Links
- Doubles up as Targeted Monitoring System
- On demand data retention, capacity exceeding several years
- Instant Analysis across thousands of Terabytes
- Correlates Identities across multiple networks
- Speaker Recognition and Target Location

[23]Paladion Networks, *Client List,* http://www.paladion.net/client_list.html
[24]Verint Systems, *Vantage,* http://www.verint.com/solutions/communications-cyber-intelligence/products/vantage/index
[25]Verint Systems, *Star-Gate,* http://www.verint.com/solutions/communications-cyber-intelligence/products/star-gate/index
[26]ClearTrail Technologies, *"Internet Monitoring Suite",* WikiLeaks, Spy Files 2011, http://www.wikileaks.org/spyfiles/docs/CLEARTRAIL-2011-Intemonisuit-en.pdf
[27]Ibid
[28]Maria Xynou, *"Spy Files 3: WikiLeaks Sheds More Light On the Global Surveillance Industry",* The Centre for Internet and Society, 25 October 2013, http://cis-india.org/internet-governance/blog/spy-files-three
[29]Ibid

2. xTrail: Targeted IP Monitoring

xTrail is a solution for interception, decoding and analysis of high speed data traffic over IP networks and independently monitors ISPs/GPRS and 3G networks. xTrail has been designed in such a way that it can be deployed within minutes and enables law enforcement agencies to intercept and monitor targeted communications without degrading the service quality of the IP network. This product is capable of intercepting all types of networks -including wireline, wireless, cable, VoIP and VSAT networks- and acts as a black box for "record and replay" targeted Internet communications[30].

Furthermore, xTrail can filter based on a "pure keyword", a URL/Domain with a keyword, an IP address, a mobile number or even with just a user identity, such as an email ID, chat ID or VoIP ID. Furthermore, xTrail can be integrated with link analysis tools and can export data in a digital format which can allegedly be presented in court as evidence.

In short, xTrail's key features include the following[31]:

- Pure passive probe
- Designed for rapid field operations at ISP/GPRS/Wi-Max/VSAT Network Gateways
- Stand-alone solution for interception, decoding and analysis of multi Gigabit IP traffic
- Portable trolley based for simplified logistics, can easily be deployed and removed from any network location
- Huge data retention, rich analysis interface and tamper proof court evidence
- Easily integrates with any existing centralized monitoring system for extended coverage

3. QuickTrail: Tactical Wi-Fi Monitoring

Some of the biggest IP monitoring challenges that law enforcement agencies face include cases when targets operate from public Internet networks and/or use encryption.

QuickTrail is a device which is designed to gather intelligence from public Internet networks, when a target is operating from a cyber cafe, a hotel, a university campus or a free Wi-Fi zone. In particular, QuickTrail is equipped with multiple monitoring tools and techniques that can help intercept almost any wired, Wi-Fi or hybrid Internet network so that a target communication can be monitored. QuickTrail can be deployed within fractions of seconds to intercept, reconstruct, replay and analyze email, chat, VoIP and other Internet activities of a target. This device supports real time monitoring and wiretapping of Ethernet LANs.[32]

According to ClearTrail's brochure, QuickTrail is a "all-in-one" device which can intercept secured communications, know passwords with c-Jack attack, alert on activities of a target, support active and passive interception of Wi-Fi and wired LAN and capture, reconstruct and replay. It is noteworthy that QuickTrail can identify a target machine on the basis of an IP address, MAC ID, machine name, activity status and several other parameters. In addition, QuickTrail supports protocol decoding, including HTTP, SMTP, POP3 and HTTPS. This device also enables the remote and central management of field operations at geographically different locations.

---

[30] ClearTrail Technologies, *"Internet Monitoring Suite"*, WikiLeaks, Spy Files 2011, http://www.wikileaks.org/spyfiles/docs/CLEARTRAIL-2011-Intemonisuit-en.pdf

[31] Maria Xynou, *"Spy Files 3: WikiLeaks Sheds More Light On the Global Surveillance Industry"*, The Centre for Internet and Society, 25 October 2013, http://cis-india.org/internet-governance/blog/spy-files-three

[32] ClearTrail Technologies, *"Internet Monitoring Suite"*, WikiLeaks, Spy Files 2011, http://www.wikileaks.org/spyfiles/docs/CLEARTRAIL-2011-Intemonisuit-en.pdf

In short, QuickTrail's key features include the following[33]:

- Conveniently housed in a laptop computer
- Intercepts Wi-Fi and wired LANs in five different ways
- Breaks WEP, WPA/WPA2 to rip-off secured Wi-Fi networks
- Deploys spyware into a target's machine
- Monitor's Gmail, Yahoo and all other HTTPS-based communications
- Reconstructs webmails, chats, VoIP calls, news groups and social networks

4. mTrail: Off-The-Air Interception

mTrail offers active and passive 'off-the-air' interception of GSM 900/1800/1900 Mhz phone calls and data to meet law enforcement surveillance and investigation requirements. The mTrail passive interception system works in the stealth mode so that there is no dependence on the network operator and so that the target is unaware of the interception of its communications[34].

The mTrail system has the capability to scale from interception of 2 channels (carrier frequencies) to 32 channels. mTrail can be deployed either in a mobile or fixed mode: in the mobile mode the system is able to fit into a briefcase, while in the fixed mode the system fits in a rack-mount industrial grade chassis.

Target location identification is supported by using signal strength, target numbers, such as IMSI, TIMSI, IMEI or MSI SDN, which makes it possible to listen to the conversation on so-called "lawfully intercepted" calls in near real-time, as well as to store all calls. Additionally, mTrail supports the interception of targeted calls from pre-defined suspect lists and the monitoring of SMS and protocol information.

In short, mTrail's key features include the following[35]:

- Designed for passive interception of GSM communications
- Intercepts Voice and SMS "off-the-air"
- Detects the location of the target
- Can be deployed as a fixed unit or mounted in a surveillance van
- No support required from GSM operator

5. Astra: Remote Monitoring and Infection framework

"Astra" is a remote monitoring and infection framework which incorporates both conventional and proprietary infection methods to ensure bot delivery to the targeted devices. It also offers a varied choice in handling the behavior of bots and ensuring non-traceable payload delivery to the controller[36].

The conventional methods of infection include physical access to a targeted device by using

---

[33]Maria Xynou, *"Spy Files 3: WikiLeaks Sheds More Light On the Global Surveillance Industry"*, The Centre for Internet and Society, 25 October 2013, http://cis-india.org/internet-governance/blog/spy-files-three

[34]ClearTrail Technologies, *"Internet Monitoring Suite"*, WikiLeaks, Spy Files 2011, http://www.wikileaks.org/spyfiles/docs/CLEARTRAIL-2011-Intemonisuit-en.pdf

[35]Maria Xynou, *"Spy Files 3: WikiLeaks Sheds More Light On the Global Surveillance Industry"*, The Centre for Internet and Society, 25 October 2013, http://cis-india.org/internet-governance/blog/spy-files-three

[36]ClearTrail Technologies, *"Internet Monitoring Suite"*, WikiLeaks, Spy Files 2011, http://www.wikileaks.org/spyfiles/docs/CLEARTRAIL-2011-Intemonisuit-en.pdf

exposed interfaces, such as a CD-ROM, DVD and USB ports, as well as the use of social media engineering techniques. However, Astra also supports bot deployment *without* requiring any physical access to the target device.

In particular, Astra can push bot to *any* targeted machine sharing the *same* LAN (wired, wi-fi or hybrid). The SEED is a generic bot which can identify a target's location, log keystrokes, capture screen-shots, capture Mic, listen to Skype calls, capture webcams and search the target's browsing history. Additionally, the SEED bot can also be remotely activated, deactivated or terminated, as and when required. Astra allegedly provides an un-traceable reporting mechanism that operates without using any proxies, which overrules the possibility of getting traced by the target.

Astra's key features include the following[37]:

- Proactive intelligence gathering
- End-to-end remote infection and monitoring framework
- Follow the target, beat encryption, listen to in-room conversations, capture keystrokes and screen shots
- Designed for centralized management of thousands of targets
- A wide range of deployment mechanisms to optimize success ration
- Non-traceable, non-detectable delivery mechanism
- Intrusive yet stealthy
- Easy interface for handling most complex tasks
- Successfully tested over the current top 10 anti-virus available in the market
- No third party dependencies
- Free from any back-door intervention

Clients

According to the data collected by the Centre for Internet and Society, the clients which are sold security solutions can include the following categories[38]:

- Law enforcement agencies / Government / Intelligence and security agencies / Police / Military / Defense
- Internet Service Providers (ISPs) / Telecom Service Providers (TSPs)
- Corporations / Organisations
- Public

The following chart illustrates the 50 companies from the random sample, the products and solutions they sell and the clients they sell them to.

Companies	**Products, Solutions and Services**	**Clients**
ClearTrail Technologies	Internet Monitoring Suite:	Law enforcement agencies

[37]Ibid

[38]Maria Xynou, *Spreadsheet data on sample of 50 security companies*, Centre for Internet and Society, 28 February 2014, http://cis-india.org/internet-governance/blog/data-on-surveillance-technology-companies

	ComTrail, xTrail, QuickTrail, mTrail, Astra	
Kommlabs Dezign	VerbaPROBE, VerbaNET, ReveaLinx (for Intelligence Agencies), Tactical (for Intelligence Agencies), VerbaCENTRE, ReveaLinx (for LEAs), Tactical (for LEAs), VerbaGATE	Law enforcement agencies, ISPs/ TSPs
Shield Security	Covert Counter Terrorist Equipment, Interception and Monitoring, Broadband and Cellular Jamming, Covert Video and Audio Systems, Body Wires, Remote Monitoring and Surveillance, Hard Wired Listening Devices, Tracking Transmitters, GPS Tracking Systems	Law enforcement agencies
Shoghi Communications	Passive A5/1 GSM Monitoring System, Semi Active GSM Monitoring, CDMA Monitoring, A5/1 Decryptor, Switch Based E1 Monitoring, Voice & Fax Logging and Analysis, Wi-Fi Interception, GSM Backhaul Monitoring Systems, Microwave Monitoring Systems, HF-VHF-UHF Monitoring System, Signal Classification and Analysis System, Satellite Geo-location, Satellite Carrier Monitoring, DCME Analysis, Inmarsat Monitoring, ISAT Monitoring, Iridium Monitoring, C/Ku-Band Satellite Link Monitoring, VSAT Monitoring, Thuraya Monitoring, Fixed Wing UAV, Rotary Wing UAV, Aerostat, ISAT Monitoring System (SCL-5032), Passive A5/1 GSM Monitoring System (SCL-5020), A5/1 Decryptor (SCL-5021)	Law enforcement agencies
Alliance Security Systems	CCTV cameras, Biometric Access Control Systems, Video Surveillance Systems	Law enforcement agencies, Corporations/ Organisations
Utimaco	Lawful Interception	Law enforcement agencies,

	Management System (LIMS): Integrates seamlessly with 250+ network nodes (switches, routers, gateways, application servers) by leading infrastructure vendors. Seamless integration with: GSM, GPRS, UMTS, LTE, PSTN, DSL, Cable,WLAN, WiMAX. Seamless integration with: GSM, GPRS, UMTS, LTE, PSTN, DSL, Cable, WLAN, WiMAX. Role-based user management, together with capability to serve different networks and law enforcement agencies concurrently, allows multiple deployment models. Components include: LIMS Management Server, LIMS Mediation Devices, LIMS Access Points, LIMS Decoder, LIMS Gateway	ISPs/ TSPs
Vehere	CommuLIM, VEHO DPI Probe, VEHO Replay, vCRIMES, vCRIMES DRS, GSMSense (portable IMSI catcher), VSIS, Dial-Log	Law enforcement agencies, ISPs/ TSPs
4Gid	4G Multi Modal ID Platform, eAccess, Enrollment devices, Authentication devices, Smart cards	Law enforcement agencies, Corporations/ Organisations
BioEnable Technology Pvt. Ltd.	Solutions specifically for Law Enforcement Agencies: (1) Crimianal Identification biometric solutions, (2) Biometric Mobile ID solutions, (3) Law Enforcement Solution - Automated Fingerprint Identification Solutions, Automated Biometric Identification Systems, Live Scan Solution, Mobile ID Solution, ID Management Prisons, ID Management for Courts, (4) Crime and Criminal Tracking Networks System (CCTNS), (5) Common Integrated Police Application	Law enforcement agencies, Corporations/ Organisations

	(CIPA), (6) Biometric Passports, (7) Biometric Security	
Fulcrum Biometrics	Biometric devices and solutions	Law enforcement agencies, Corporations/ Organisations
Iritech Inc.	Biometric hardware and software products	Law enforcement agencies, Corporations/ Organisations
Raviraj Technologies	Biometric access control products, Biometric time attendance recorders, Biometrics Identification Authentication, USB Fingerprint Scanner, Fingerprint Car Lock, Fingerprint Modules, Fingerprint Software products, Fingerprint Scanners	Law enforcement agencies
Smartmatic	(Biometric) Election Solutions and ID Management Solutions	Law enforcement agencies
Spy Action India	Spy Cameras, Spy Wireless Cameras, GPS trackers, Spy software, CCTV cameras, Spy gadgets, Spy Keylogger Software, Computer Spy software	Law enforcement agencies
Nerve Centrex	Network video surveillance cameras, video management software and wireless video networks.	Law enforcement agencies, Corporations/ Organisations
Aurora Integrated Systems (AIS)	UAVs: Urban View and Altius Mk-II, Aerostat systems: SkyView 50, SkyView 100 HD and SkyView 200	Law enforcement agencies
Speck Systems	UAVs and micro-UAVs	Law enforcement agencies
Aeron Systems	UAVs	Law enforcement agencies
Smart Avionics Co. Pvt. Ltd.	UAVs	Law enforcement agencies
Aerobot	UAVs	Law enforcement agencies
Infoserve India Pvt. Ltd.	Call Data Record (CDR) Miner application, Deep Eye Network Surveillance System, Internet Monitoring System	Law enforcement agencies
WSS Security Solutions Pvt. Ltd.	CCTV cameras	Law enforcement agencies, Corporations/ Organisations
Verint Systems	Impact 360 Speech Analytics, Impact 360 Text Analytics, Nextiva Video Management	Law enforcement agencies, Corporations/ Organisations

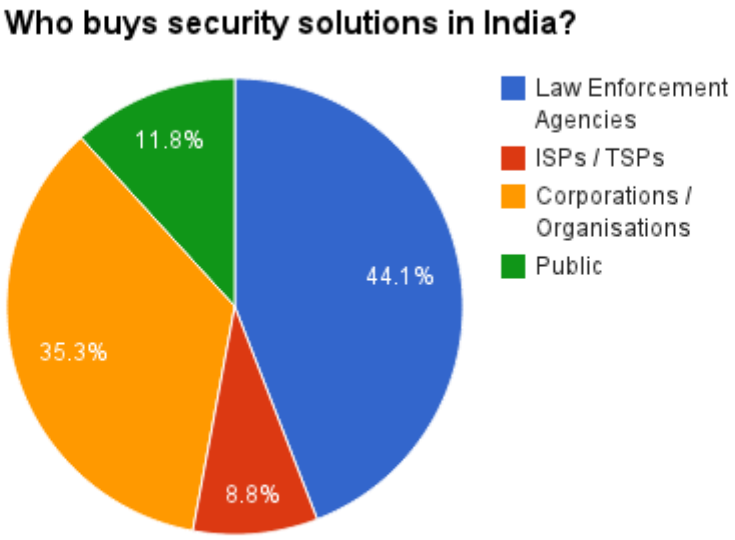
	Software (VMS), Nextiva Physical Security Information Management (PSIM), Nextiva Network Video Recorders (NVRs), Nextiva Video Business Intelligence (VBI), Nextiva Surveillance Analytics, Nextiva IP cameras, CYBERVISION Network Security, ENGAGE suite, FOCAL-INFO (FOCAL-COLLECT & FOCAL-ANALYTICS), RELIANT, STAR-GATE, VANTAGE, Audiolog for Public Safety, Impact 360 for Public Safety	
AGC Networks	IP surveillance cameras, video analytics, access control systems, automatic vehicle number plate recognition system	Law enforcement agencies, Corporations/ Organisations
Aqsacom	(1) AQSACOM Lawful Interception Management System: ALIS (2) AQSACOM's Data Retention Intelligence Solution: ADRIS	Law enforcement agencies, ISPs/ TSPs
Paladion Networks	(1) Internet Monitoring System, (2) Monitoring of Landline and Cellphone Networks, (3) Unified Monitoring Platform, (4) Portable Monitoring Device, (5) Cyber Cafe Monitoring, (6) SSL Interception and Decryption Systems, (7) Hand Held Wifi Monitoring, (8) Remote Desktop / Laptop Monitoring, (9) Granular Webpages Blocking, (10) Link Analysis, (11) Computer and Cellphone Forensics	Law enforcement agencies, ISPs/ TSPs
Polaris Wireless	Altus: phone monitoring, location monitoring and analytics	Law enforcement agencies
Polixel Security Systems	Face Recognition System, Automatic Number Plate Recognition System, Video Analytics, Voting Card	Law enforcement agencies
Pyramid Cyber Security	SIP based Video IP Phones and cameras, Video Analytics,	Law enforcement agencies

	CCTV surveillance cameras and 360° Panoramic Cameras, Access Control Systems	
XenArmor	Network SSL Certificate Scanner, Advanced Keylogger Detector, Network Attack Detector, Universal Password Recovery Kit, Windows Password Recovery services & Cyber Crime Investigation services	Law enforcement agencies, Corporations/ Organisations
Span Technologies	2002: VoIP for ILD operations in the carrier segment 2003: Lawful Monitoring solutions among Indian ILD operators 2004: Wimax 2005: Web/email acceleration solutions & SIP telephony 2006: Converged TDM and IP monitoring & Broadband over Power Lines 2007: GSM backhaul optimization & QOS over IP networks 2008: Introduction of IMS & Location Based Services Platform 2009: Antispam for SMS and Email 2010: Digital Repeaters, Converged Multi-service Gateway and Internet Bandwidth Optimization, Broadband/ IP based Services/ VAS to TELCOS and ISPs in the SAARC region i.e. India, Bangladesh, Sri Lanka, Nepal and Bhutan 2011: Lawful Interception for 3G and 4G Networks, Hosted Audio and Video conferencing services and Office in a Box solution	ISPs/ TSPs
Amsan Technology	CCTV Cameras, Wireless Systems Camera, IP Cameras, Access Control Systems, Biometric Machines	Corporations/ Organisations
Sterling CCTV Solutions	CCTV cameras and access control systems	Corporations/ Organisations

Aimansys Technologies	CCTV cameras and biometric access control systems	Corporations/ Organisations
Navtel Tech. Inc.	Access management solutions, asset & vehicle tracking, video surveillance solutions	Corporations/ Organisations
Data Outsourcing India	Data mining services	Corporations/ Organisations
Cynosure Technologies Pvt. Ltd. (Timelabs)	Biometric devices & Face Recognition Systems	Corporations/ Organisations
Spy Impex	Spy cameras, phone monitoring software and GPS vehicle tracking systems	Corporations/ Organisations, Public
Aryabhatta Infosys	Biometric devices, RFID, Access Control Systems, Voice Recognition, Face Recognition Systems	Corporations/ Organisations
Savant Automation	CCTV cameras, Access control systems, RFID solutions	Corporations/ Organisations, Public
Icon Infosystems	Voice Recognition software, Call recording and monitoring solutions	Corporations/ Organisations, Public
Spy Action India	Spy Cameras, Spy Wireless Cameras, GPS trackers, Spy software, CCTV cameras, Spy gadgets, Spy Keylogger Software, Computer Spy software	Corporations/ Organisations, Public
Convexicon Software Solutions India Pvt. Ltd.	Vehicle Tracking Systems (software and hardware), Biometric Access Control Systems, CCTV cameras	Corporations/ Organisations
Incept	CCTV cameras and biometric access control systems	Corporations/ Organisations
Mobile Spy India (Retina-X studios)	Spy Software for mobile phones	Public
Nice Deal	Spy Hidden Cameras, GPS Trackers and Navigators, Call Monitoring Devices, Spy Wall Listening Devices, Spy Bluetooth Watches, Pen Drive Voice Recorders, 3G Wireless Cameras, Hidden Security Cameras, Spy Mobile Software	Public
Action India	Spy Cameras (including Spy Keychain Camera, Spy Glasses Camera, Spy Wrist Watch Camera, and many others), Spy	Public

	Wireless Cameras (including Spy 3G Hidden Camera), 2-way GSM Audio Listening Device, Digital Voice Recorder, Spy USB Voice Recorder, Spy Wall Listening Device, Spy Voice Recorder Pen, Spy Hidden Mobile Battery GSM BUG, Spy Mobile Phone Software, Spy Key Logger, Spy GPS Tracker Watch Mobile, Spy Walky-talky Watches, Mobile Watch Phone, Spy Watch Mobile Phone, Spy GPS Vehicle Tracker, Spy GPS Personal Tracker, Spy GPS Mobile Tracker, Spy GPS Tracker Watch Mobile	
Adisys Technologies Pvt. Ltd.	CCTV cameras, CCTV DVR, IP cameras, Access Control Systems	Corporations/ Organisations
SilverStar Tracking Solutions	Vehicle Trackers	Public
Legend Systems Private Limited (Precision Biometric)	Fingerprint Devices, Iris, BioNIX, InnaIT-CBS, UID Kit, InnaIT-SDK, FI Kit, Attendance and Access Control Systems	Corporations/ Organisations

The following pie chart illustrates the above with regards to the clients that buy security solutions.



From the random sample of 50 security companies, the majority of these companies (44.1%) appear to sell products and solutions to law enforcement agencies, intelligence and security agencies, the military and to the police. For example, many of these companies sell CCTV cameras to the police, unmanned aerial vehicles (UAVs) to the Indian military, biometric systems to the Unique Identification Authority of India (UIDAI) and possibly even phone and Internet monitoring systems to intelligence agencies. Many companies (35.3%) from the sample sell security solutions to corporations and organisations, such as CCTV cameras or access control systems to hotels or businesses.

Few companies (11.8%) from the sample appear to sell solutions to Internet Service Providers (ISPs) and Telecom Service Providers (TSPs). It is noteworthy though that all companies that have ISPs/ TSPs as clients sell Internet and phone monitoring solutions, which are not always restricted to targeted surveillance. Lastly, only 8.8% of the companies in the sample appear to sell products to the public. Such companies sell relatively cheap surveillance cameras and various spy products, which can theoretically be purchased by anyone who can afford them[39].

While the chart provides an idea of who most security solutions are sold to, it is not necessarily representative for the whole of India or for the entire security industry in the country, since it is only based on a random sample. However, the above chart does indicate that law enforcement and security agencies appear to have the most vested interest in security solutions, which can be verified by the fact that they are officially responsible for tackling crime and terrorism.

Compliance with Lawful Regulations and Standards, Certifications and Privacy Policies

Companies which produce and sell security solutions are urged to comply with lawful regulations and standards, to be certified and to include privacy policies in their websites. This provides a minimal assurance that such products are legally regulated, that their security has been tested and that such companies provide data protection to their customers.

[39]Ibid

Lawful Regulations and Standards

Several international lawful regulations and standards have been created over the last decades and companies that produce security solutions should comply with them.

Many security companies across the world comply with standards created by such organisations. From the second research sample of 50 security companies operating in India, only the following 6 companies have public information about company compliance with lawful regulations and standards:

1. ClearTrail Technologies
2. Kommlabs Dezign
3. Utimaco
4. Vehere
5. Verint Systems
6. Aqsacom

It is noteworthy that out of these 6 companies, only half of them are Indian (ClearTrail Technologies, Kommlabs Dezign and Vehere), while the other three have international headquarters (Utimaco, Verint Systems and Aqsacom). In other words, 44 companies from the random sample of 50 companies do not publish information about whether or not they comply at all with any lawful regulations and standards, while only 3 out of 40 Indian companies appear to do so.

Examples of lawful regulations and standards include:

Alliance for Telecommunications Industry Solutions (ATIS)

The American National Standards Institute (ANSI) accredited the Alliance for Telecommunications Industry Solutions (ATIS), which is a standards organisation that has more than 250 member companies, including various telecommunications service providers (TSPs), equipment manufacturers and vendors[40]. As such, ATIS includes numerous industry committees which discuss, evaluate and author guidelines related to data security, network reliability, technological interoperability and subscription services. ATIS is also a founding member of the Global Standards Collaboration, as well as a founding partner of the Third Generation Partnership Project (3GPP), which is a collaboration between groups of telecommunications associations[41].

European Telecommunications Standards Institute (ETSI)

The European Telecommunications Standards Institute (ETSI) produces global standards for information and communications technologies (ICT), including fixed, mobile, radio, converged, broadcast and Internet technologies. ETSI is officially recognised by the European Union as a European Standards Organisation for ICT and encompasses more than 700 ETSI member organisations in 62 countries across the world[42].

ETSI produces a variety of standards in response to market demand, including the following:

- European Standard (EN)

[40] Alliance for Telecommunications Industry Solutions (ATIS), *About ATIS*, http://www.atis.org/about/index.asp
[41] Ibid
[42] European Telecommunications Standards Institute (ETSI), *About ETSI*, http://www.etsi.org/about

- ETSI Standard (ES)
- ETSI Guide (EG)
- ETSI Technical Specification (TS)
- ETSI Special Report (SR)
- ETSI Group Specification (GS)

Most security companies around the world choose to comply with ETSI standards because they are considered to have a very high quality. Since its establishment in 1998, ETSI has produced more than 30,000 standards that enable global technologies such as GSM, 3G, 4G, DECT and smart cards[43]. Such standards address the needs for interconnection and interoperability, ensure safety, reliability and environmental care and protect user and business interests, in support of government policies[44].

Communications Assistance for Law Enforcement Act (CALEA)

The Communications Assistance for Law Enforcement Act (CALEA) was passed in 1994 in the United States and expands the ability of law enforcement agencies to conduct electronic surveillance by requiring telecommunications carriers to have built-in surveillance capabilities in their equipment, facilities and services[45]. CALEA has expanded to include all VoIP and broadband Internet traffic and the wiretapping and interception of communications in the United States is usually conducted under this Act[46].

According to CALEA, communications service providers in the United States are required to purchase and install new hardware and software which meets the surveillance requirements of law enforcement agencies. Furthermore, communications service providers are also required to modify old equipment, so that it enables law enforcement agencies to conduct real-time surveillance on telecommunications and Internet traffic. As CALEA includes a list of requirements for surveillance, many security companies around the world comply with them. In particular, CALEA encompasses a list of assistance capability requirements, according to which telecommunications carriers are required to assist law enforcement agencies in intercepting and wiretapping communications. These requirements include the following[47]:

- Interception of communications
- Access to call-identifying information
- Delivery of information and communications to law enforcement agencies
- Provision of privacy and security of communications and unobtrusive interception
- Provision of mobile service assistance
- Decryption capability
- Monitoring by law enforcement at TSP premise during an emergency or an exigent circumstance
- Specific industry design (of monitoring equipment) is *not* required
- Industry change is *not* prohibited

Although CALEA does not specify technologies or standards that carriers must meet in the above

[43]European Telecommunications Standards Institute (ETSI), *Our Standards,* http://www.etsi.org/standards
[44]European Telecommunications Standards Institute (ETSI), *Why we need standards,* http://www.etsi.org/standards/why-we-need-standards
[45]FCC, *"Summary of CALEA requirements"*, TIA TR45 Lawfully Authorised Electronic Surveillance, Cryptome, 16 November 2002, Version 2.1., http://cryptome.org/laes/calea-require.pdf
[46]Electronic Frontier Foundation, *FAQ on the CALEA expansion by the FCC,* https://www.eff.org/pages/calea-faq#11
[47]FCC, *"Summary of CALEA requirements"*, TIA TR45 Lawfully Authorised Electronic Surveillance, Cryptome, 16 November 2002, Version 2.1., http://cryptome.org/laes/calea-require.pdf

requirements, it does contain a "safe harbor" provision. Lawmakers insert "safe harbor" provisions in statutes when the desired compliance goals can not be codified in the law. As such, the CALEA safe harbor provision is created through a technical standard-setting process[48]. However, CALEA does not rely on law enforcement to create a set of standards, but on the industry. In particular, Section 107(a) (2) of CALEA states that if a communications carrier complies with *"publicly available technical requirements or standards adopted by an industry association or standard-setting organisation"*, the government will consider it to be compliant with CALEA[49]. In short, the six companies from the random sample that comply with CALEA likely comply with standards that have been created by the industry, rather than by law enforcement.

All 6 companies that comply with the ANSI standards comply with the European Telecommunications Standards Institute (ETSI) standards and with the Communications Assistance for Law Enforcement Act (CALEA) legal requirements, while only Utimaco and Aqsacom appear to additionally comply with the 3GPP and ATIS standards.

Certification Standards

Companies that provide security solutions should be certified by an accredited organisation, in order to ensure that their equipment has been tested. Out of the 50 companies in the random research sample, 19 companies have publicly available information about certification from information available on their websites. In other words, 31 companies out of the research sample do not publish information about the certification standards that they adhere to.

The companies from the random research sample which publish certification information include the following:

1. Kommlabs Dezign (ISO 9001: 2008, ISO 27001: 2005)
2. Shoghi Communications (ISO 9001: 2008)
3. Alliance (ISO 9001: 2000)
4. Vehere (ISO 9001:2008, ISO 27001: 2005)
5. 4Gid Solutions (ISO 9001: 2008)
6. BioEnable (ISO 9001: 2000, ISO 9001: 2008)
7. Incept (STQC certification, INCITS 379, ISO 19794-6)
8. Raviraj Technologies (STQC certification, FBI, PIV, CE, FCC)
9. Nerve Centrex (ISO 9001:2008)
10. Speck Systems (ISO 9001, ISO 27001)
11. Infoserve (ISO 9001:2008)
12. Convexicon (ISO 9001:2008)
13. Verint systems (ISO 9001:2008, 27001: 2007, 14001:2004)
14. AGC Networks (ISO 9001:2008, ISO 27001:2005)
15. Aqsacom (ISO 9001: 2001)
16. Paladion Networks (CISSP, CISA, SANS, BS7799, CSCP, ISO 200000, ISO 27001)
17. Polixel (ISO 9001: 2008)
18. Pyramid Cyber Security (ISO 9001: 2008, ISO 27001: 2005)
19. Precision Biometric (STQC certification, ISO 9001: 2008, BioApi)

It is evident from the above list that almost all of these companies are ISO certified. In particular, the International Organisation for Standardization, known as ISO, is an international standard-

[48]Subsention: To Notice Secretly, *CALEA "Safe Harbor" in four easy steps*, 22 October 2013, http://www.subsentio.com/live/regulatory/joels-blog-time/safe-harbor-review-20131022/

[49]Electronic Frontier Foundation, *FAQ on the CALEA expansion by the FCC*, https://www.eff.org/pages/calea-faq#11

setting body which consists of representatives from national standards organisations. ISO was founded in 1947 and as it produces worldwide proprietary, industrial and commercial standards, many corporations and organisations around the world comply with them[50].

Out of the 19 certified companies from the random research sample, 7 companies appear to be ISO 27001 certified. The ISO 27001 standards are created for "Information security management" and help organisations and corporations "manage the security of assets such as financial information, intellectual property, employee details" or information entrusted to them by third parties[51]. Similarly to other ISO management system standards, ISO 27001 certification is not mandatory. As such, the remaining 12 companies that are not ISO 27001 certified may potentially ensure the security of the data they handle through technological means, though this remains unclear.

It is noteworthy that almost all of the certified companies in the random research sample are ISO 9001 certified. The ISO 9000 standards are created for the purpose of "Quality Management" to ensure that products and services meets customer's requirements and that their quality is consistently improved. The ISO 9001: 2008 standards set out the requirements of a quality management system and are the only ISO 9000 standards that companies can be certified to. More than one million companies and organisations in over 170 countries are ISO 9001: 2008 certified. This certification includes Quality Management Principles, as well as the requirement for regular internal audits of the quality management systems of ISO 9001: 2008 certified companies. Such audits can be performed by independent certification bodies which can verify a company's conformity with the certification standard, or by clients[52]. Concisely, the Quality Management Principles of the ISO 9001: 2008 certification standard include the following[53]:

- Customer focus
- Leadership
- Involvement of people
- Process approach
- System approach to management
- Continual improvement
- Factual approach to decision making
- Mutually beneficial supplier relationships

Almost all of the certified companies in the random research sample are ISO 9001: 2008 certified and potentially comply with the above principles for the quality management of their products, solutions and services.

India seeks to become a certifying nation

The 2013-2014 Standing Committee on Information Technology issued the 52nd Report on "Cyber Crime, Cyber Security, and Right to Privacy", which highlights India's need to reform its cyber security framework and to establish privacy legislation. This Report also states that India seeks to become a certifying nation for electronic products in terms of security testing. The Indian Common Criteria Certification Scheme (IC3S) which is operated by the STQC Directorate was successfully audited and by becoming a certifying nation, India will issue certificates that will be valid across the

[50]International Organisation for Standardization (ISO), *About ISO*, http://www.iso.org/iso/home/about.htm
[51]International Organisation for Standardization (ISO), *Standards: ISO/IEC 27001 – Information security management"*, http://www.iso.org/iso/home/standards/management-standards/iso27001.htm
[52]International Organisation for Standardization (ISO), *Standards: ISO 9000 – Quality management*, http://www.iso.org/iso/home/standards/management-standards/iso_9000.htm
[53]International Organisation for Standardization (ISO), *"Quality Management Principles"*, 2012, http://www.iso.org/iso/qmp_2012.pdf

globe. As such, products tested and certified under India's Common Criteria Certification Scheme will be acceptable in other countries around the world, without re-testing them[54].

The STQC Directorate has established an infrastructure and made the operational testing and certification of the security of IT products as per the Common Criteria Standards (ISO 15408) for evaluation up to an assurance level of EAL4. On behalf of the Department of Electronics and Information Technology (DEITY), STQC has signed the Common Criteria Recognition Arrangements (CCRA). However, the present scope of certification is limited to Network Boundary Protection Devices and General Purpose Operating Systems, but India aims to expand its capacity and capability for testing and certification as per the Common Criteria Standards. STQC currently lacks the knowledge and expertise for highly complex products, such as radar, but hopes to share its knowledge on Common Criteria standards and methodology with other organisations[55].

Privacy Policies

A privacy policy is a legal statement which specifies some or all of the ways with which a party collects, uses, discloses, shares, retains and manages a client's data. The 50 companies in the random research sample handle client's data and sell products and solutions which also handle individual's personal data by third parties. As such, it was deemed interesting to examine whether these companies include privacy policies on their websites.

Out of the 50 companies from the random research sample, only 19 companies appear to have privacy policies on their websites. These companies include the following[56]:

1. Shield Security
2. Shoghi Communications
3. Utimaco
4. Vehere
5. 4Gid
6. Adisys
7. Fulcrum Biometrics
8. Incept
9. Spy Impex
10. Spy Action India
11. Speck Systems Ltd.
12. Infoserve
13. SilverStar Tracking Solutions
14. Convexicon
15. Verint Systems
16. Aqsacom
17. Paladion Networks
18. Polaris Wireless
19. Polixel

It is noteworthy that out of these 19 companies, 7 of them have international headquarters (Shield

[54]Standing Committee on Information Technology (2013-2014), *"Fifty-second Report on Cyber Crime, Cyber Security, and Right to Privacy"*, Ministry of Communications and Information Technology, Department of Electronics and Information Technology, Government of India, Fifteenth Lok Sabha, New Delhi, 12 February 2014, http://164.100.47.134/lsscommittee/Information%20Technology/15_Information_Technology_52.pdf

[55]Ibid

[56]Maria Xynou, *Spreadsheet data on sample of 50 security companies*, Centre for Internet and Society, 28 February 2014, http://cis-india.org/internet-governance/blog/data-on-surveillance-technology-companies

Security, Utimaco, Fulcrum Biometrics, Verint systems, Aqsacom, Polaris Wireless and Polixel), while only 12 out of the 40 Indian companies of the random research sample appear to include privacy policies on their websites. Since only 19 companies in total appear to provide privacy policies, 31 companies from the random research sample do not appear to legally define how they handle their clients personal data[57].

3.3. Ranking Security Companies

As part of the research on the random sample of 50 security companies operating in India, these companies were evaluated based on their potential for harm on human rights and civil liberties. In particular, the 50 companies were evaluated based on two main criteria:

- Their products and solutions
- Their clients

The first evaluation criterion (products and solutions) was chosen because a company's potential to affect individual's human rights can possibly be judged based on the type of products and solutions that it sells. The second evaluation criterion (clients) was chosen because the harm potential of a product or solution depends, to some degree, on who it is sold to. In other words, the 50 companies of this random research sample were ranked and evaluated based on what type of products and solutions they sell and who they have stated they sell them to.

Ranking Security Solutions

The solutions produced and sold by the 50 companies of the random research sample fall within the following ten categories:

1. Internet monitoring software
2. Data mining and profiling software
3. Phone monitoring software
4. Speech analysis / Voice recognition software
5. Face recognition software
6. Location monitoring software/ hardware
7. Analytics
8. Visual surveillance (e.g. CCTV cameras)
9. Aerial surveillance (e.g. Drones)
10. Biometric (access control) systems

The harm potential (on human rights) of the above categories has been evaluated based on the following three criteria:

1. Outreach (mass or targeted surveillance)
2. Type of data captured
3. Amount of data captured

Law enforcement agencies carry out the lawful interception of communications in democratic regimes when such surveillance is targeted and includes a judicial warrant or other authorisation[58]. Mass surveillance, however, can lack a warrant for every individual case of interception and as

[57] Ibid

[58] European Telecommunications Standards Institute (ETSI), *Lawful Interception*, http://www.etsi.org/technologies-clusters/technologies/security/lawful-interception

such, the potential for abuse appears to be much higher in instances of mass surveillance than in targeted surveillance. Furthermore, unlike targeted surveillance, it is much more challenging to prove the necessity, adequacy and proportionality of the mass interception of communications[59]. Therefore, the probability of breach is much higher in cases of mass surveillance and as such, the solutions produced by the 50 companies of the sample have been evaluated based on whether they carry out targeted or mass surveillance. In other words, according to the first criterion (outreach), solutions are ranked based on how many people they potentially affect.

The second criterion evaluates the companies' solutions based on the types of data they capture. While it is undoubtedly a challenging task to evaluate the various types of data, especially since their significance varies depending on context and many other variables, the Centre for Internet and Society has attempted to broadly evaluate the significance of various types of data depending on how identifiable they potentially are to an individual. In particular, certain types of solutions are designed in a way which enables them to capture specific types of data, which potentially identify an individual much more accurately than other types of solutions. For example, a biometric access control system is designed to capture a relatively limited amount of data, such as fingerprints and other personal information linked to them, while spyware which can remotely be deployed in a computer can potentially capture everything in the target's machine, ranging from photos and sketches to personal confidential documents[60]. As such, it is evident that certain security solutions appear to have the potential to affect human rights depending on the type of data they capture.

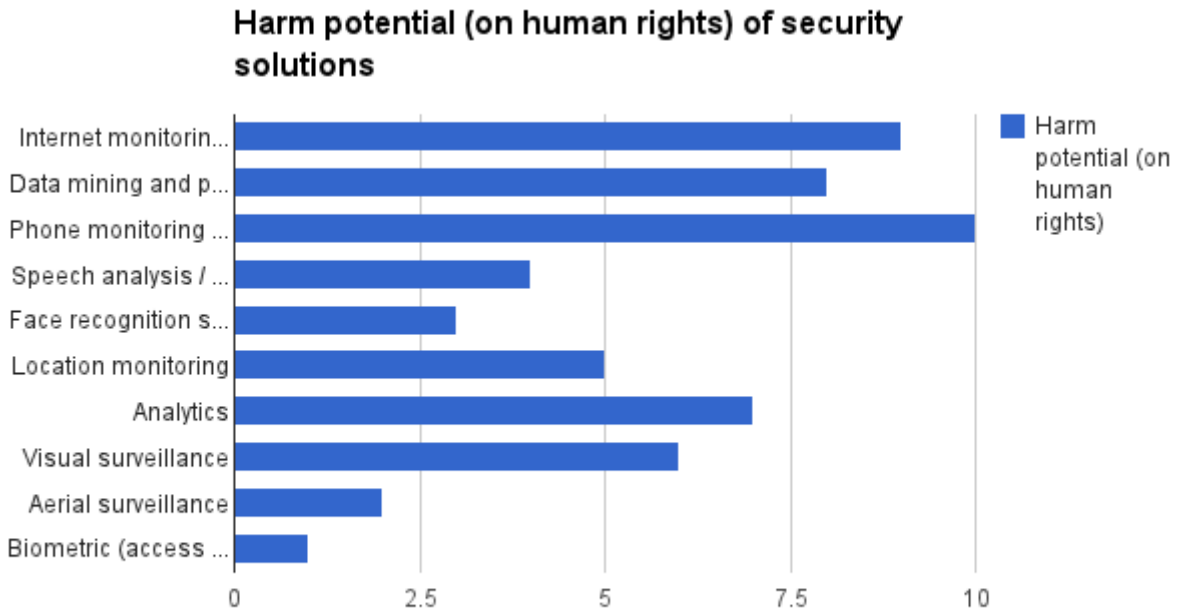
The third and final criterion evaluates the 50 companies' solutions based on the amount of data they capture. For example, spyware which is deployed into an activist's computer may be used for targeted purposes[61], but may potentially have more severe effects on that individual's human rights than other mass surveillance technologies. As such, regardless of whether a solution carries out mass or targeted surveillance, the amount of data it captures once it's being used appears to have some value. Therefore, the amount of data captured by security solutions sold by these 50 companies is used as an evaluation criterion.

Based on the above three evaluation criteria for security solutions, the categories of solutions have been ranked on a scale of 1-10, where those ranked 1 exhibit the least potential for harm (on human rights) and those ranked 10 exhibit the most. The following chart illustrates the ranking:

[59]Electronic Frontier Foundation, Privacy International & Access, *"International Principles on the Application of Human Rights to Communications Surveillance"*, Necessary & Proportionate, 10 July 2013, https://www.eff.org/files/necessaryandproportionatefinal.pdf

[60]ClearTrail Technologies, *"Internet Monitoring Suite"*, WikiLeaks, Spy Files 2011, http://www.wikileaks.org/spyfiles/docs/CLEARTRAIL-2011-Intemonisuit-en.pdf

[61]Alinda Vermeer, *"Surveillance follows Ethiopian political refugee to the UK"*, Privacy International, 17 February 2014, https://www.privacyinternational.org/blog/surveillance-follows-ethiopian-political-refugee-to-the-uk



According to the above chart, phone monitoring solutions are ranked with the most potential for harm on human rights (ranked 10), while biometric (access control) systems are ranked with the least potential for harm (ranked 1). Based on the three evaluation criteria for the types of solutions, Internet monitoring and phone monitoring solutions appear to have the greatest outreach (since they are potentially used by communications carriers for mass surveillance), and can potentially capture huge volumes of various types of data.

Phone monitoring solutions in India appear to have a greater potential for harm than internet monitoring solutions due to the following reasons:

- 73% of India's population uses mobile phones, while only 17% has access to the Internet[62]
- Many Indians have access to the Internet through their mobile phones and thus phone monitoring solutions can capture *both* call data and Internet data
- Governmental surveillance schemes, such as the Central Monitoring System (CMS), target telecommunications (it remains unclear if they target Internet communications) through TSPs[63]

As such, it is evident that the outreach of phone monitoring solutions is potentially greater than that of Internet monitoring solutions, especially since the vast majority of India's population uses mobile phones, whereas a small percentage of the population has regular access to the Internet[64]. Therefore, mass surveillance in India is probably carried out mostly through the interception of mobile communications, rather than Internet communications. While the amount and types of data captured in both cases are hard to evaluate accurately, it is likely that they are similar. Phone monitoring (PM) solutions were ranked higher (10) than Internet monitoring (IM) solutions (9) due to the following:

(1) PM Outreach > IM Outreach
(2) PM Types of Data ~ IM Types of Data

[62]We are Social, *India*, 2014 Edition, http://wearesocial.net/tag/india/
[63]Maria Xynou, *"India's Central Monitoring System (CMS): Something to Worry About?"*, Centre for Internet and Society, 30 January 2014, http://cis-india.org/internet-governance/blog/india-central-monitoring-system-something-to-worry-about
[64]We are Social, *India*, 2014 Edition, http://wearesocial.net/tag/india/

(3) PM Volume of Data ~ IM Volume of Data

Thus PM > IM.

Internet monitoring solutions encompass a wide range of various types of software and hardware, including spyware which can remotely be deployed into a target's computer (such as ClearTrail's QuickTrail product) and public network monitoring solutions[65]. As such, internet monitoring solutions appear to entail a much broader category of software than data mining and profiling software, which can potentially have a greater outreach and capture larger volumes of various types of data. Data mining and profiling software undoubtedly analyse large volumes of data, but usually such data has been captured by other internet monitoring solutions. Hence, internet monitoring (IM) solutions have been ranked higher (9) than data mining and profiling (DMP) software (8) due to the following:

(1) IM Outreach > DMP Outreach
(2) IM Types of Data > DMP Types of Data
(3) IM Volume of Data > DMP Volume of Data

Thus IM > DMP.

While data mining and profiling software and data analytics may appear to be rather similar, they are actually different with regards to their scope, purpose and focus of analysis. In particular, data analytics are used to examine raw data with the purpose of drawing conclusions about that information, to verify or disprove existing models or theories and involve confirmatory data analysis (CDA). Data mining software, on the other hand, sorts through large data sets with the use of artificial intelligence and uncovers hidden patterns and relationships. As such, data mining software involves exploratory data analysis (EDA), as sophisticated software is used to uncover and match patterns through vast volumes of data.[66] Data mining and profiling (DMP) software is ranked higher (8) than data analytics (DA) software (7) due to the following:

(1) DMP Outreach > DA Outreach
(2) DMP Types of Data > DA Types of Data
(3) DMP Volume of Data > DA Volume of Data

Thus DMP > DA.

Data analytics appear to have a greater outreach than visual surveillance solutions, such as CCTV cameras, since they can potentially analyse much vaster amounts of data and have the potential to match patters and draw conclusions[67] – which most visual surveillance solutions do not. Once data is captured through visual surveillance solutions, it is usually further processed by data analytics. However, data analytics is a broad field and can include various other types of data, beyond those captured by visual surveillance solutions. As such, data analytics (DA) software is ranked higher (7) than visual surveillance (VS) solutions (6) due to the following:

(1) DA Outreach > VS Outreach
(2) DA Types of Data > VS Types of Data
(3) DA Volume of Data > VS Volume of Data

[65] ClearTrail Technologies, *"Internet Monitoring Suite"*, WikiLeaks, Spy Files 2011, http://www.wikileaks.org/spyfiles/docs/CLEARTRAIL-2011-Intemonisuit-en.pdf
[66] Margaret Rouse, *"Data Analytics (DA)"*, Tech Target, Data Management, 10 January 2008, http://searchdatamanagement.techtarget.com/definition/data-analytics
[67] Ibid

Thus DA > VS.

Visual surveillance solutions are ranked higher than location monitoring solutions because the first have the potential to capture more categories of data than the second. For example, a CCTV camera can capture data including an individual's location, acquaintances, habits and other information, whereas location monitoring solutions may possibly be limited to an individual's location – and other information potentially linked to it. Furthermore, visual surveillance solutions are more often installed for mass monitoring purposes, whereas location monitoring solutions are often used for targeted surveillance. As such, visual surveillance (VS) solutions are ranked higher (6) than location monitoring (LM) solutions (5) due to the following:

(1) VS Outreach > LM Outreach
(2) VS Types of Data > LM Types of Data
(3) VS Volume of Data ~ LM Volume of Data

Thus VS > LM.

Location monitoring solutions are ranked with a greater potential for harm (on human rights) than speech analysis and voice recognition software, because the second is used for targeted purposes and analyses a specific amount of data. Location monitoring solutions, however, are capable of capturing broader categories of data, while speech analysis/voice recognition software is a tool used for analysing data captured by other solutions[68]. Therefore, location monitoring (LM) solutions are ranked higher (5) than speech analysis/voice recognition (SA/VR) software (4) due to the following:

(1) LM Outreach > SA/VR Outreach
(2) LM Types of Data > SA/VR Types of Data
(3) LM Volume of Data ~ SA/VR Volume of Data

Thus LM > SA/VR.

Both speech analysis/voice recognition and face recognition software appear to be rather similar, since they analyse specific data captured through targeted surveillance. However, speech analysis/voice recognition software has been ranked higher than face recognition software because the first analyses data captured through phone monitoring (which is ranked with the greatest potential for harm), whereas the second type of software analyses data captured through visual surveillance (ranked far below phone monitoring). As such, since phone monitoring (PM) has been ranked (above) with a greater harm potential than visual surveillance (VS), speech analysis/voice recognition (SA/VR) software, which analyses data captured through phone monitoring, appears to have a greater harm potential (4) than face recognition (FR) software (3). In short, the following derives from the above:

PM > IM > DMP > DA > VS (=) PM > VS
PM (SA/VR) > VS (FR) (=) SA/ VR > FR

Thus SA/VR > FR.

Similarly, face recogntion and aerial surveillance (in the instance of non-weaponised drones) also

[68]Maria Xynou, *Spreadsheet data on sample of 50 security companies*, Centre for Internet and Society, 28 February 2014, http://cis-india.org/internet-governance/blog/data-on-surveillance-technology-companies

appear to fall within broader categories of surveillance. In particular, face recognition software belongs to the broader category of visual surveillance (VS) solutions, while non-weaponised aerial surveillance appears to fall within the broader category of location monitoring (LM) solutions. As such, face recognition (FR) software appears to have a greater harm potential on human rights (3) than non-weaponised aerial surveillance (AS) solutions (2) due to the following:

VS > LM (=) VS (FR) > LM (AS) (=) FR > AS

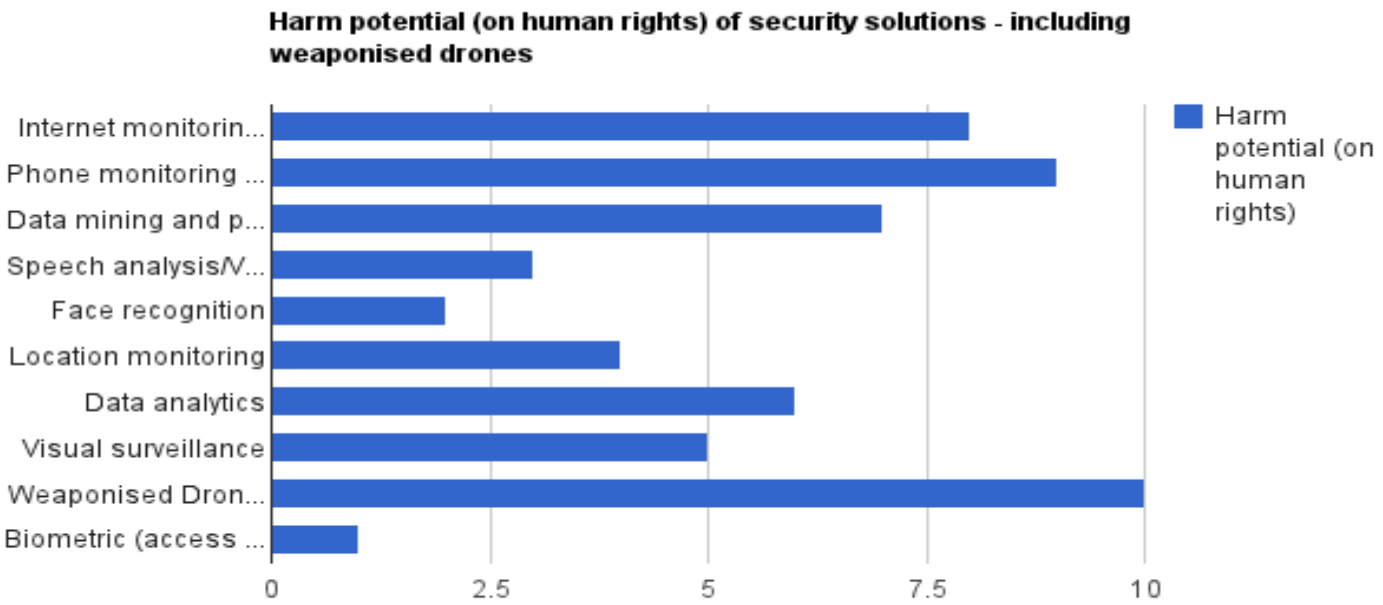
Thus FR > AS.

Lastly, non-weaponised aerial surveillance solutions appear to have a greater harm potential than biometric (access control) systems. The first category is based on other types of data which have previously been captured by other solutions (such as location monitoring), whereas the second category does not necessarily require the prior collection of data by other, more "harmful", solutions since it gathers data on a primary basis. Furthermore, such primary data is usually restricted to biometrics and does not expand to other, broader categories of data[69]. Therefore, non-weaponised aerial surveillance (AS) solutions appear to have a greater harm potential (2) than biometric (access control) systems (BS) (1) due to the following:

LM > SA/VR > FR > AS (=) LM (AS) > BS (=) AS > BS

Thus AS (non-weaponised) > BS.

However, in the instance of weaponised drones, the above change completely. In particular, weaponised drones have the potential to deprive individuals of their right to life, which is the greatest fundamental human right. As such, weaponised drones undoubtedly have the greatest harm potential than all other security solutions and are ranked 10, as illustrated in the following chart:



[69]Ibid

Ranking Clients

The 50 companies from the random research sample appear to sell security solutions to the following categories of clients[70]:

- Law enforcement agencies / Governments / Intelligence Agencies / Security Agencies / Police / Military / Defense
- Internet Service Providers (ISPs) / Telecom Service Providers (TSPs)
- Corporations / Organisations
- Public

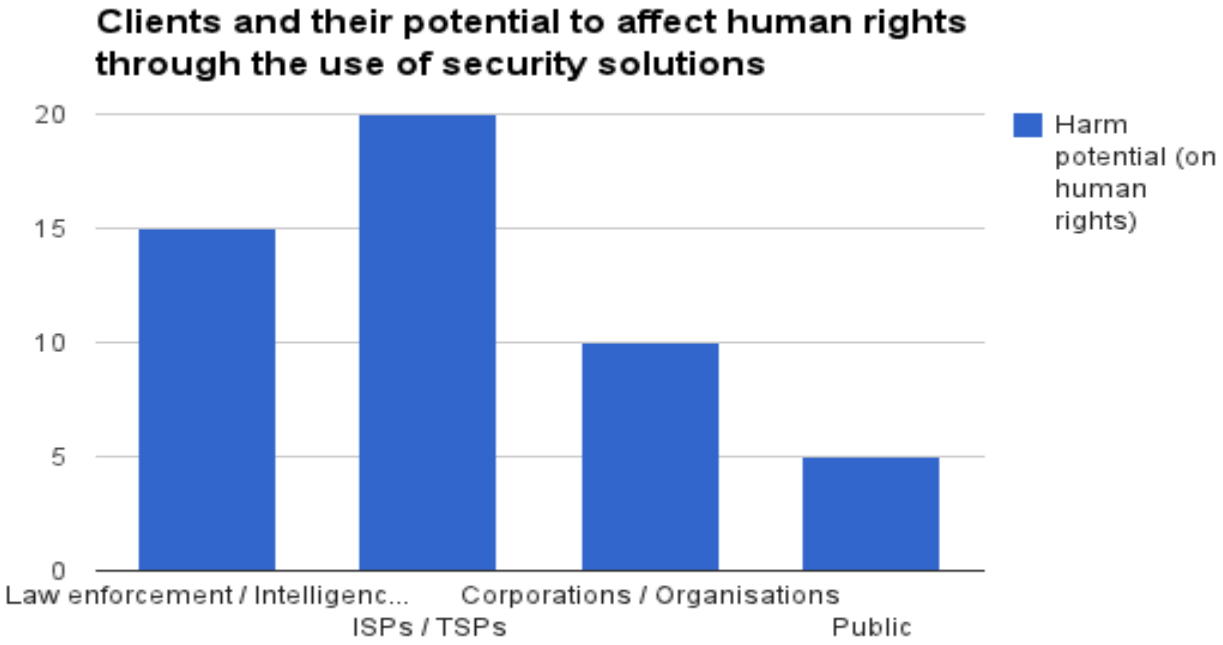
The above categories have been ranked based on the following three criteria:

1. Authority
2. Access to data
3. Interception capabilities

In particular, the categories of clients are ranked based on the amount of authority they have to legally collect, access, share, disclose and retain data. This criterion has been chosen because it determines the power that the clients have over the data they handle and hence the amount of power they have to potentially affect individual's right to privacy and other human rights. The second criterion involves the amount of data that clients have access to. Clients which have access to larger and vaster volumes of data potentially have a higher probability of affecting individual's human rights. The third criterion involves the client's potential power to carry out the interception of communications. As such, clients which have more authority over mass data, more access to large volumes of data and the power to intercept communications potentially have a higher probability of breaching such data – especially if adequate safeguards are not in place.

The above categories of clients have been ranked on a scale of A-D (A=5, B=10, C=15, D=20), where A represents the least potential for harm (on human rights), while D represents the most potential for harm. The following chart illustrates the clients and their potential to affect human rights in India, through the use of security solutions sold to them by the 50 companies in the random sample:

[70] Ibid



According to the above chart, it is evident that ISPs/TSPs appear to have the greatest potential to affect human rights in India through the use of security solutions (ranked D), while the public appears to have the least potential to affect human rights by purchasing security solutions (ranked A).

ISPs/ TSPs have been ranked higher than law enforcement agencies because, while the second category may have legal authority over the handling of intercepted data and the power to potentially prosecute individuals, the first category of service providers has both direct access to large volumes of data (through internet and phone monitoring which are highly ranked, as mentioned previously) and the direct power to intercept communications running through its networks. As such, ISPs / TSPs appear to have a greater potential to affect human rights (ranked D) through the use of security solutions than law enforcement agencies (LEAs) (ranked C) due to the following:

(1) ISPs/ TSPs Authority < LEAs Authority
(2) ISPs / TSPs Access to Data > LEAs Access to Data
(3) ISPs / TSPs Interception Capabilities > LEAs Interception Capabilities

Thus ISPs / TSPs > LEAs.

However, this ranking may potentially change, as the Indian Government's Central Monitoring System (CMS) aims at bypassing service providers and at collecting intercepted data at central and regional databases[71]. In this instance, law enforcement agencies potentially have a greater harm potential than communications service providers, but that depends on whether they will have access to mass volumes of data, or on whether their access will be restricted to targeted cases. This currently remains unclear, which is why service providers have currently been ranked with a greater harm potential.

Through access to intercepted data by ISPs and TSPs, law enforcement agencies have access to

[71]Maria Xynou, *"India's Central Monitoring System (CMS): Something to Worry About?"*, Centre for Internet and Society, 30 January 2014, http://cis-india.org/internet-governance/blog/india-central-monitoring-system-something-to-worry-about

larger volumes of data than corporations and organisations, as well as the legal authority to handle such data and to potentially prosecute individuals based on it. In certain instances, law enforcement agencies have interception capabilities, which corporations and organisations lack. Therefore, the category of law enforcement agencies (LEAs) appears to have a greater potential to affect human rights (ranked C) through the use of security solutions than corporations and organisations (Corps) (ranked B) due to the following:

(1) LEAs Authority > Corps Authority
(2) LEAs Access to Data > Corps Access to Data
(3) LEAs Interception Capabilities > Corps Interception Capabilities

Thus LEAs > Corps.

It is noteworthy that solutions bought by corporations / organisations and the public are restricted to the lower ranking solutions (with the least potential for harm), since they lack the authority, capability and incentive to use mass interception systems, such as phone and internet monitoring solutions. The public is included as a category because some of the companies in the sample sell various spy products, such as coca-cola spy cameras, to anyone who can afford to purchase them. According to the research sample, corporations and organisations on the other hand tend to widely purchase CCTV cameras and biometric (access control) systems[72]. Neither corporations and organisations nor the public have authority over data or any legal interception capabilities. As such, these two categories have been compared and ranked merely on their access to data.

Corporations and organisations, such as hotels and businesses, appear to have a greater potential to affect human rights than the public as a client category, because they tend to handle and have access to larger amounts of data. An individual which purchases a spy product, such as a SpyWatch, probably has access to a very limited amount of third data, while a national bank, for example, operating a biometric (access control) system for all its employees undoubtedly has access to and handles larger amounts of data. Therefore, corporations and organisations (Corps) appear to have a greater potential to affect human rights (ranked B) through the use of security solutions than the public (PUB) as a client (ranked A) due to the following:

Corps Access to Data > PUB Access to Data (=) Corps > PUB

Ranking Security Companies

The harm potential of the 50 companies of the random research sample has been evaluated based on the following two criteria:

- Security solutions
- Clients

As such, each of the 50 companies have been evaluated based on the types of solutions that they produce and the clients that they sells them to. The ranking for each of the 50 companies can be viewed analytically through Appendix 3. Additionally, the chart at the end of this sub-chapter illustrates the ranking of these companies. In particular, Kommlabs Dezign is ranked with the greatest potential for harm on human rights (based on the solutions is produces and the clients it sells them to), followed by Vehere and Paladion Networks. It is noteworthy that, while the random sample consists of 10 foreign security companies, the top 3 companies with the greatest potential

[72]Maria Xynou, *Spreadsheet data on sample of 50 security companies*, Centre for Internet and Society, 28 February 2014, http://cis-india.org/internet-governance/blog/data-on-surveillance-technology-companies

for harm appear to be Indian. Precision Biometric is ranked last, with the least potential for harm on human rights.

The accuracy of this ranking may potentially be widely debated on, especially with regards to the various ranking criteria. However, the aim of this research is to broadly illustrate the industrial surveillance actors in India and in particular: who sells surveillance technologies. By identifying some of the main industrial surveillance actors in India, it is hence easier to identify, examine and analyse the various surveillance schemes being implemented in the country. The objective of this research is to enable further in-depth research in India on its surveillance regime.

Furthermore, it should be pointed out that this research does not aim to criticise certain companies and/or clients as "harmful" per se. The data sample was randomly selected to reduce the probability of bias towards specific companies. Additionally, all data collected about these companies was gathered from their websites and from other publicly available sources.

The purpose of this data collection is to illustrate a portion of the security industry in India and of some of its actors, in order to enable further research on surveillance. The objective behind the ranking is to point out the variety within the security companies and to illustrate that some of their security solutions may potentially affect individual's right to privacy and other human rights.

Policy Recommendations and Conclusion

While security solutions may potentially aid law enforcement agencies in tackling crime and terrorism, they also present a high potential for abuse. In particular, the unlawful and unregulated use of surveillance technologies which have the capability of capturing individual's personal data without their knowledge or consent may potentially pose a major threat to their right to privacy and other human rights. In general, the unlawful collection of, access to and sharing of personal data can potentially result in data breaches and hence violations to human rights.

Activists and political dissidents can be the primary targets of some of the most sophisticated surveillance technologies, even though their use is supposed to be limited to so-called criminals and terrorists. Privacy International recently reported that an Ethiopian political refugee in the UK was targeted by FinFisher spyware, as the trojan was detected in his computer[73]. In May 2013, Mac OS X spyware, signed with a valid Apple Developer ID, was detected on the laptop of an Angolan activist at a human rights conference in Norway[74]. As such, it is evident that some governments around the world purchase surveillance technologies not only to track criminals and terrorists, but to also potentially spy on activists and political dissidents.

The following policy recommendations work to ensure that Indians human rights are protected in light of an expanding surveillance industry.

Regulation of Security Solutions

Surveillance is not unregulated in India. On the contrary, the various laws which regulate surveillance in India were analysed in Chapter 1. However, none of the existing laws appear to

[73]Alinda Vermeer, *"Surveillance follows Ethiopian political refugee to the UK"*, Privacy International, 17 February 2014, https://www.privacyinternational.org/blog/surveillance-follows-ethiopian-political-refugee-to-the-uk

[74]Lucian Constantin, *"Developer-signed Mac spyware found on Angolan activist's computer"*, Macworld, 17 May 2013, http://www.macworld.com/article/2038960/developer-signed-mac-spyware-found-on-angolan-activists-computer.html

regulate the various types of security solutions, but vaguely require law enforcement agencies to carry out the interception of communications in certain instances – as stated in Section 69 of the Information Technology (Amendment) Act, 2008, for example[75].

International regulations and standards, such as the ETSI standards[76] and CALEA legal requirements[77], are in place and many security companies around the world comply with them. While it is encouraged for companies to comply with such standards and regulations, they may potentially inadequately regulate the various types of security solutions, especially since most standards are created by the industry, rather than by law enforcement. As such, many of these standards may not necessarily be in compliance with the Justice AP Shah privacy principles[78] and with the International Principles on the Application of Human Rights to Communications Surveillance[79], and may therefore potentially allow for data breaches. Furthermore, such standards and regulations do not explicitly regulate the various types of security solutions, and nor are they legally binding.

Companies are encouraged to certify their security solutions, to ensure information security[80] and the quality of their products[81]. Additionally, all security companies should include privacy policies on their websites in order to legally state how they handle their customers data. While compliance with certification standards and the inclusion of privacy policies on websites are a decisive step in protecting individuals personal data, they might not be adequate in preventing data breaches by various surveillance technologies.

The contemporary reality of surveillance appears to entail various types of security solutions, all of which should not be broadly regulated under a vague "interception umbrella". The previous sub-chapters illustrated that not all security solutions have the same potential for harm on human rights. Certain security solutions, such as internet and phone monitoring software, appear to have a greater harm potential than other solutions, such as CCTV cameras and biometric access control systems. Furthermore, not all security solutions are used by the same clients for the same purpose, or under the same type of authorisation. As such, the various types of security solutions should be explicitly regulated depending on their harm potential.

In particular, it is recommended that the Information Technology (Amendment) Act, 2008[82], is

[75]The Information Technology (Amendment) Act, 2008, http://police.pondicherry.gov.in/Information%20Technology%20Act%202000%20-%202008%20%28amendment%29.pdf

[76]European Telecommunications Standards Institute (ETSI), *Our Standards*, http://www.etsi.org/standards

[77]FCC, *"Summary of CALEA requirements"*, TIA TR45 Lawfully Authorised Electronic Surveillance, Cryptome, 16 November 2002, Version 2.1., http://cryptome.org/laes/calea-require.pdf

[78]Justice Ajit Prakash Shah, Former Chief Justice, High Court of Delhi, *"Report of the Group of Experts on Privacy"*, Planning Commission (CIT&I Division), Government of India, 16 October 2012, http://planningcommission.nic.in/reports/genrep/rep_privacy.pdf

[79]Electronic Frontier Foundation, Privacy International & Access, *"International Principles on the Application of Human Rights to Communications Surveillance"*, Necessary & Proportionate, 10 July 2013, https://www.eff.org/files/necessaryandproportionatefinal.pdf

[80]International Organisation for Standardization (ISO), *Standards: ISO/IEC 27001 – Information security management"*, http://www.iso.org/iso/home/standards/management-standards/iso27001.htm

[81]International Organisation for Standardization (ISO), *Standards: ISO 9000 – Quality management*, http://www.iso.org/iso/home/standards/management-standards/iso_9000.htm

[82]The Information Technology (Amendment) Act, 2008, http://police.pondicherry.gov.in/Information%20Technology%20Act%202000%20-%202008%20%28amendment%29.pdf

amended to include provisions for security solutions, which should be in compliance with the Justice AP Shah privacy principles[83] and with the International Principles on the Application of Human Rights to Communications Surveillance[84]. New clauses should be added to the Information Technology (Amendment) Act, 2008, which should:

- specify the *types of security solutions* which can be legally used for the purpose of national security or for the investigation of a crime or offense
- specify the *parties which can legally use* such security solutions for the purpose of national security or for the investigation of a crime or offense
- specify that the use of such security solutions should only be authorised by an independent and competent judicial authority, once the necessity, adequacy and proportionality of such use has been adequately proven

In addition to the above, the various security solutions should be categorised and regulated based on their ranking, as analysed in the previous sub-chapters. In particular, phone monitoring and Internet monitoring solutions have been ranked with the highest harm potential on human rights and as such, it is recommended that they are separately regulated. Additional clauses should be included in the Information Technology (Amendment) Act, 2008[85], which regulate the various types of "intrusion software" and "network surveillance systems", as those sold by companies such as ClearTrail Technologies, Paladion Networks and Kommlabs Dezign[86]. Such regulations should:

- limit the instances according to which such solutions can be used to extreme cases of national security, once their necessity, adequacy and proportionality has been adequately proven in court
- guarantee safeguards for individuals, in compliance with the principles of notice, choice and consent
- specify the limited instances according to which individual consent should not or can not be acquired
- should prohibit the unauthorised sharing and disclosure of collected data
- be in compliance with the principles of collection limitation and purpose limitation
- specify and limit the retention period of collected data according to the period necessary for an investigation
- require the complete destruction of collected data once its retention period has expired
- impose strict penalties in instances of breach

The Department of Telecommunications of the Ministry of Information Technology and Communications in India has issued guidelines for surveillance and communications service providers are required to comply with them[87]. However, such guidelines are not legally binding, which is why it is highly recommended that the specific use of solutions with a high harm potential,

[83]Justice Ajit Prakash Shah, Former Chief Justice, High Court of Delhi, *"Report of the Group of Experts on Privacy"*, Planning Commission (CIT&I Division), Government of India, 16 October 2012, http://planningcommission.nic.in/reports/genrep/rep_privacy.pdf

[84]Electronic Frontier Foundation, Privacy International & Access, *"International Principles on the Application of Human Rights to Communications Surveillance"*, Necessary & Proportionate, 10 July 2013, https://www.eff.org/files/necessaryandproportionatefinal.pdf

[85]The Information Technology (Amendment) Act, 2008, http://police.pondicherry.gov.in/Information%20Technology%20Act%202000%20-%202008%20%28amendment%29.pdf

[86]Maria Xynou, *"Big democracy, big surveillance: India's surveillance state"*, OpenDemocracy, 10 February 2014, http://www.opendemocracy.net/opensecurity/maria-xynou/big-democracy-big-surveillance-indias-surveillance-state

[87]Yatish Yadav, *"New Guidelines Formulated for Monitoring, Interception of Phone Calls"*, The New Indian Express, 11 January 2014, http://www.newindianexpress.com/nation/New-Guidelines-Formulated-for-Monitoring-Interception-of-Phone-Calls/2014/01/11/article1994336.ece#.Uw6GUZh_W8Y

such as phone monitoring and internet monitoring software and hardware, should be legally regulated. Such regulations should be in compliance with the Justice AP privacy principles[88] and with the International Principles on the Application of Human Rights to Communications Surveillance[89].

Additionally, the Department of Telecommunications (DoT) requires communications service providers to purchase specific types of solutions. However, the DoT does not appear to be transparent about these types of solutions. The Centre for Internet and Society (CIS) sent a Right To Information (RTI) request to the DoT, requesting a list of all of the security solutions that it requires communications service providers to purchase, install and use. The DoT, though, denied to disclose this information on the grounds of national security. The value of knowing what type of solutions are being used by law enforcement is grounded in the assumption that various solutions have different harm potential. For example, if the DoT authorises and requires the use of mass monitoring solutions, citizens should have the right to be informed so that they can ensure that the right checks and balances are in place.

Non-transparency with regard to potentially harmful to human rights technologies should not be acceptable in a democratic regime. As such, it is recommended that the Information Technology (Amendment) Act, 2008, is amended in compliance with the principle of transparency[90] and that a clause is added which requires law enforcement to inform Indian citizens about the types of security solutions that are being used.

Export and Import Controls of Surveillance Technologies

Certain types of security solutions which are sold in the international market, such as FinFisher spyware produced by Gamma Group[91], appear to present a threat to human rights. As previously mentioned, FinFisher spyware was recently detected in the computer of an Ethiopian political refugee in the UK[92]. Similarily, some of ClearTrail's solutions, such as QuickTrail, can remotely be deployed into a computer, intercept data and monitor communications[93]. As such, it is evident that spyware which is designed to remotely and secretly be deployed into a target's computer and capture all personal data presents a threat to privacy and other human rights.

Privacy International has demanded that surveillance technologies are treated as the weapons of the digital age, since they potentially pose a threat to human rights, and that their export is controlled[94]. It is suggested that similar export controls in India, especially since some of its companies, such as Kommlabs Dezign, Vehere, Paladion Networks and ClearTrail Technologies, produce solutions

[88]Justice Ajit Prakash Shah, Former Chief Justice, High Court of Delhi, *"Report of the Group of Experts on Privacy"*, Planning Commission (CIT&I Division), Government of India, 16 October 2012, http://planningcommission.nic.in/reports/genrep/rep_privacy.pdf

[89]Electronic Frontier Foundation, Privacy International & Access, *"International Principles on the Application of Human Rights to Communications Surveillance"*, Necessary & Proportionate, 10 July 2013, https://www.eff.org/files/necessaryandproportionatefinal.pdf

[90]Ibid

[91]Morgan Marquis-Boire, Bill Marczak, Claudio Guarnieri & John Scott-Railton, *"For Their Eyes Only: The Commercialization of Digital Spying"*, The Citizen Lab, 30 April 2013, https://citizenlab.org/2013/04/for-their-eyes-only-2/

[92]Alinda Vermeer, *"Surveillance follows Ethiopian political refugee to the UK"*, Privacy International, 17 February 2014, https://www.privacyinternational.org/blog/surveillance-follows-ethiopian-political-refugee-to-the-uk

[93]ClearTrail Technologies, *"Internet Monitoring Suite"*, WikiLeaks, Spy Files 2011, http://www.wikileaks.org/spyfiles/docs/CLEARTRAIL-2011-Intemonisuit-en.pdf

[94]Sophie Curtis, *"Privacy International threatens legal action over surveillance tech exports"*, TechWorld, 25 July 2012, http://news.techworld.com/security/3372104/privacy-international-threatens-legal-action-over-surveillance-tech-exports/

which present a high harm potential to human rights[95].

Membership in Multilateral Export Control Regimes

On an international level, significant progress has recently been marked with regards to export controls of surveillance technologies[96]. In particular, the following two new categories of surveillance have been added to the control list of the Wassenaar Arrangement:

- Intrusion software
- IP network surveillance systems

The first category was proposed by the UK and aims at controlling "Advanced Persistent Threat Software and related equipment (offensive cyber tools)", which includes malware and rootkits, such as FinFisher (sold by Gamma Group) and Da Vinci (sold by Hacking Team) spyware. The second category was proposed by France and aims at controlling general traffic analysis systems, such as Deep Packet Inspection (DPI) items[97].

The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies is a multilateral export control regime with 41 participating states, currently excluding India[98]. However, India has applied to join membership of four multilateral export control regimes: the Nuclear Suppliers Group (NSG), the Missile Technology Control Regime (MTCR), the Australia Group and the Wassenaar Arrangement. Generally, member countries harmonise their national systems in accordance with the new mechanisms of these regimes. If India joins these regimes it will have the advantage of participating in the management of the global commerce of advanced technology[99]. Furthermore, if India gains membership in the Wassenaar Arrangement, it will also have to control the export of the new aforementioned categories of surveillance: intrusion software and IP network surveillance systems. As such, India's membership in this Arrangement, to ensure that potentially intrusive technologies are better controlled is encouraged.

National Export and Import Controls of Surveillance Technologies

The Foreign Trade (Development and Regulation) Act (FTDR), 1992[100], is India's primary law for its trade control system. This Act empowers the Directorate General of Foreign Trade to license the export and import of items on the Indian Tariff Classification (Harmonised System) list, which is divided into two schedules: one for imports and one for exports[101].

The Indian government expanded the scope of its trade controls with the passage of the Weapons of

[95] View Appendix 3.

[96] Edin Omanovic, *"International agreement reached controlling export of mass and intrusive surveillance technology"*, Privacy International, 09 December 2013, https://www.privacyinternational.org/blog/international-agreement-reached-controlling-export-of-mass-and-intrusive-surveillance

[97] Ibid

[98] *The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies and Munitions List*, WA-LIST (13) 1, 04 December 2013, http://www.wassenaar.org/controllists/2013/WA-LIST%20%2813%29%201/WA-LIST%20%2813%29%201.pdf

[99] Rajiv Nayan, *"Update on India's Membership of Multilateral Export Control Regimes"*, Institute for Defense Studies and Analyses, 19 December 2012, http://idsa.in/idsacomments/UpdateonIndiasMembershipofMultilateralExportControlsRegimes_rnayan_191212

[100] *FTDR Act, 1992 and Foreign Trade Policy,* Unit 8, http://nbaindia.org/uploaded/Biodiversityindia/Legal/29.%20Foreign%20Trade%20%28Development%20and%20Regulation%29%20Act,%201992.pdf

[101] SECURUS Strategic Trade Solutions, *"India's Export Controls: Current Status and Possible Changes on the Horizon"*, 10 July 2011, http://www.securustrade.com/India%27s%20Export%20Controls_Article__July_10_2011_FINAL.pdf

Mass Destruction and Their Delivery Systems (Prohibition of Unlawful Activities) Act in 2005. This Act regulates the export, re-transfer, re-export, transit, and transhipment of any items related to the development, production, handling, operation, maintenance, storage or dissemination of weapons of mass destruction. Additionally, controls are established on the trade of other sensitive items such as firearms, explosives, nuclear substances and chemicals through the following[102]:

- Atomic Energy Act, 1962
- Chemical Weapons Convention Act, 2000
- Arms Act, 1959

However, goods, technologies and services subject to export licensing requirements are listed in India's national dual-use export control list, known as the Special Chemicals, Organisms, Materials, Equipment, and Technologies (SCOMET) list. The SCOMET list is a legal document notified under the Foreign Trade (Development and Regulation) Act, 1922, it is divided into eight categories of items (Categories 0-7) and the Directorate General of Foreign Trade is the primary licensing authority[103]. However, the SCOMET list does not appear to be fully consistent with the multilateral export control regimes, such as the NSG, MTCR, Australia Group and Wassenaar Arrangement lists[104].

It could be useful for India to amend the SCOMET list to include the export control of intrusive – to human rights – surveillance technologies. In particular, the SCOMET list could be amended similarly to the Wassenaar Arrangement to include controls for two new categories: "intrusive software" and "network surveillance systems"[105]. Through the export control of these two additional categories, companies such as ClearTrail Technologies can potentially be prevented from exporting mass surveillance systems, such as ComTrail, to repressive regimes[106]. Furthermore, it is recommended that the licensing conditions with regards to these additional categories are specified and that they are further examined by an independent authority.

India's import licensing system is substantially less developed than its controls on exports. In particular, the Indian government only requires a license for imports of the following sensitive items[107]:

- nuclear and radiological materials, including irradiated fuel elements of nuclear reactors, heavy water, other nuclear fuels, inorganic and organic compounds of rare earth metals, uranium ores, and related substances
- selected hydrocarbons and derivative substances from countries that are not parties to the Montreal Protocol
- CWC-listed chemicals, some organic chemicals, hazardous chemicals, and pesticides
- explosives, including gunpowder and detonators
- aircraft and spacecraft

---

[102]Ibid

[103]V.K. Srivastava & Arvind Madhavan, *"India's Export Control System: Inter-Agency Cooperation and Coordination"*, 20th Asian Export Control Seminar, Tokyo, 2012, http://www.simul-conf.com/outreach/2012/asian_ec/2-C2%20Mr%20Madhavan%20&%20Mr%20Srivastava%20%28India%29.pdf

[104]SECURUS Strategic Trade Solutions, *"India's Export Controls: Current Status and Possible Changes on the Horizon"*, 10 July 2011, http://www.securustrade.com/India%27s%20Export%20Controls_Article__July_10_2011_FINAL.pdf

[105]Edin Omanovic, *"International agreement reached controlling export of mass and intrusive surveillance technology"*, Privacy International, 09 December 2013, https://www.privacyinternational.org/blog/international-agreement-reached-controlling-export-of-mass-and-intrusive-surveillance

[106]ClearTrail Technologies, *"Internet Monitoring Suite"*, WikiLeaks, Spy Files 2011, http://www.wikileaks.org/spyfiles/docs/CLEARTRAIL-2011-Intemonisuit-en.pdf

[107]SECURUS Strategic Trade Solutions, *"India's Export Controls: Current Status and Possible Changes on the Horizon"*, 10 July 2011, http://www.securustrade.com/India%27s%20Export%20Controls_Article__July_10_2011_FINAL.pdf

- warships
- nickel and articles thereof
- conventional arms and ammunition

The Directorate General of Foreign Trade and designated Regional Authorities license imports of most restricted items[108]. It would be useful for "intrusive software" and "network surveillance systems" to be added on the import control list, in order to prevent the import of intrusive spyware, such as FinFisher and Da Vinci, to India. Additionally, it is recommended that the licensing conditions with regards to these additional categories are specified and that they are further examined by an independent authority.

Establishment of a Surveillance Oversight Committee

It is also important that the principle of public oversight is implemented and enforced.[109] This could be through the establishment of a Surveillance Oversight Committee in India, in addition to the existing Review Committee. Such a committee could be comprised of individuals with the following designations:

- Technologists / Security researchers (with a specialisation in malware analysis and artificial intelligence, among others)
- Lawyers (experienced in export/import controls, IT and privacy law)
- Privacy experts

The objective behind the establishment of such a committee would be to create an independent authority which will ensure that:

- Agencies using security solutions are doing so lawfully
- The use of security solutions is in compliance with the Justice AP Shah privacy principles[110], and with the International Principles on the Application of Human Rights to Communications Surveillance[111]
- Agencies which misuse security solutions or which use unlawful or unauthorised solutions are held accountable
- Security solutions used in India are evaluated based on their potential to infringe upon human rights
- The Department of Telecommunications is transparent and publishes the list of required and authorised security solutions
- The conditions for licensing the import and export of restricted items are in compliance with Indian laws and human rights
- Regular security checks are in place to prevent the use of solutions which have a high potential to infringe upon human rights

Through the establishment of an independent authority, such as a Surveillance Oversight Committee, the general use or misuse of security solutions will be monitored, cases of breach will

[108]Ibid

[109]Electronic Frontier Foundation, Privacy International & Access, *"International Principles on the Application of Human Rights to Communications Surveillance"*, Necessary & Proportionate, 10 July 2013, https://www.eff.org/files/necessaryandproportionatefinal.pdf

[110]Justice Ajit Prakash Shah, Former Chief Justice, High Court of Delhi, *"Report of the Group of Experts on Privacy"*, Planning Commission (CIT&I Division), Government of India, 16 October 2012, http://planningcommission.nic.in/reports/genrep/rep_privacy.pdf

[111]Electronic Frontier Foundation, Privacy International & Access, *"International Principles on the Application of Human Rights to Communications Surveillance"*, Necessary & Proportionate, 10 July 2013, https://www.eff.org/files/necessaryandproportionatefinal.pdf

be addressed and authorities will be held accountable. Thus, the potential for abuse may be reduced, while better safeguards for Indian's right to privacy and other human rights will potentially be ensured.

References

Alinda Vermeer, *"Surveillance follows Ethiopian political refugee to the UK"*, Privacy International, 17 February 2014, https://www.privacyinternational.org/blog/surveillance-follows-ethiopian-political-refugee-to-the-uk

Alliance for Telecommunications Industry Solutions (ATIS), *About ATIS*, http://www.atis.org/about/index.asp

Aman Sharma, *"NATGRID to get legal powers soon"*, The Economic Times, 10 September 2013, http://articles.economictimes.indiatimes.com/2013-09-10/news/41938113_1_executive-order-national-intelligence-grid-databases

Aman Sharma, *"NATGRID to get running in 4 months"*, The Economic Times, 07 December 2013, http://articles.economictimes.indiatimes.com/2013-12-07/news/44909645_1_databases-national-counter-terrorism-centre-information-security

Amiti Sen & Harsimran Julka, *"India seeks 'Data Secure Nation' status, more Hi-end business from European Union"*, The Economic Times, 16 April 2012, http://articles.economictimes.indiatimes.com/2012-04-16/news/31349813_1_data-security-council-data-protection-laws-standard-contractual-clauses

BBC News Technology, *"India is 'ready to use' BlackBerry message intercept system"*, 11 July 2013, http://www.bbc.co.uk/news/technology-23265091

Bhairav Acharya, *"Comments on the Proposed Rule 138A of the Central Motor Vehicle Rules, 1989, Concerning Radio Frequency Identification Tags"*, The Centre for Internet and Society, 03 December 2012, http://cis-india.org/internet-governance/blog/comments-on-motor-vehicle-rules

Bhairav Acharya, *"Comments on the Information Technology (Guidelines for Cyber Cafe) Rules, 2011"*, The Centre for Internet and Society, 31 March 2013, http://cis-india.org/internet-governance/blog/comments-on-the-it-guidelines-for-cyber-cafe-rules-2011

Bhairav Acharya, *"Comments on the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011"*, The Centre for Internet and Society (CIS), 31 March 2013, http://cis-india.org/internet-governance/blog/comments-on-the-it-reasonable-security-practices-and-procedures-and-sensitive-personal-data-or-information-rules-2011

Bhairav Acharya, *"Privacy (Protection) Bill, 2013: Updated Third Draft"*, The Centre for Internet and Society, 30 September 2013, http://cis-india.org/internet-governance/blog/privacy-protection-bill-2013-updated-third-draft

Central Bureau of Investigation – India, *MLATs*, http://cbi.nic.in/interpol/mlats.php

Centre for Internet and Society (CIS), *Presentation on MLATs*, http://cis-india.org/internet-governance/blog/presentation-on-mlats.pdf

Centre for Internet and Society, *Surveillance Industry: Table 1*, 02 May 2013, http://cis-india.org/internet-governance/blog/table-1.pdf

Centre for Internet and Society, *Surveillance Industry: Table 2*, 02 May 2013, http://cis-india.org/internet-governance/blog/table-2.pdf

Centre for Internet and Society, *Brief Material for Honourable MOC & IT Press Briefing on 16.07.2013*, http://cis-india.org/internet-governance/blog/new-cms-doc-2

CIOL Bureau, *"Government's Central Monitoring System to be operational soon"*, 11 March 2013, http://www.ciol.com/ciol/news/184770/governments-central-monitoring-system-operational-soon

ClearTrail Technologies, *"Internet Monitoring Suite"*, WikiLeaks, Spy Files 2011, http://www.wikileaks.org/spyfiles/docs/CLEARTRAIL-2011-Intemonisuit-en.pdf

CNN Library, *"Mumbai Terror Attacks"*, 19 September 2013, http://edition.cnn.com/2013/09/18/world/asia/mumbai-terror-attacks/

Deccan Herald, *"MHA seeks over Rs. 3,400 crore for NATGRID"*, 29 January 2014, http://www.deccanherald.com/content/181065/mha-seeks-over-rs-3400.html

Deepa Kurup, *"In the dark about 'India's PRISM'"*, The Hindu, 16 June 2013, http://www.thehindu.com/sci-tech/technology/in-the-dark-about-indias-prism/article4817903.ece

Delta Bureau, *"Crime Tracking Easier with CCTNS"*, The Hindu, Tamil Nadu, 18 September 2013, http://www.thehindu.com/news/national/tamil-nadu/crime-tracking-easier-with-cctns/article5141371.ece

DNA India, *"NATGRID begins operations; high security protocols deployed"*, 22 December 2013, http://www.dnaindia.com/india/report-natgrid-begins-operations-high-security-protocols-deployed-1939160

DNA India, *"Government issues standard operating procedures for phone-tapping in India"*, 10 January 2014, http://www.dnaindia.com/india/report-government-issues-standard-operating-procedures-for-phone-tapping-in-india-1948730

Edin Omanovic, *"International agreement reached controlling export of mass and intrusive surveillance technology"*, Privacy International, 09 December 2013, https://www.privacyinternational.org/blog/international-agreement-reached-controlling-export-of-mass-and-intrusive-surveillance

Electronic Frontier Foundation, Privacy International & Access, *"International Principles on the Application of Human Rights to Communications Surveillance"*, Necessary & Proportionate, 10 July 2013, https://www.eff.org/files/necessaryandproportionatefinal.pdf

Electronic Frontier Foundation, *FAQ on the CALEA expansion by the FCC*, https://www.eff.org/pages/calea-faq#11

Elonnai Hickok, *"Draft International Principles on Communications Surveillance and Human Rights"*, The Centre for Internet and Society, 16 January 2013, http://cis-india.org/internet-governance/blog/draft-intl-principles-on-communications-surveillance-and-human-rights

ET Bureau, *"NATGRID to take off soon on home ministry data"*, The Economic Times, 17 January 2014, http://articles.economictimes.indiatimes.com/2014-01-17/news/46301449_1_natgrid-the-national-intelligence-grid-home-ministry

European Telecommunications Standards Institute (ETSI), *About ETSI*, http://www.etsi.org/about

European Telecommunications Standards Institute (ETSI), *Our Standards*, http://www.etsi.org/standards

European Telecommunications Standards Institute (ETSI), *Why we need standards*, http://www.etsi.org/standards/why-we-need-standards

European Telecommunications Standards Institute (ETSI), *Lawful Interception*, http://www.etsi.org/technologies-clusters/technologies/security/lawful-interception

FCC, *"Summary of CALEA requirements"*, TIA TR45 Lawfully Authorised Electronic Surveillance, Cryptome, 16 November 2002, Version 2.1., http://cryptome.org/laes/calea-require.pdf

FTDR Act, 1992 and Foreign Trade Policy, Unit 8, http://nbaindia.org/uploaded/Biodiversityindia/Legal/29.%20Foreign%20Trade%20%28Development%20and%20Regulation%29%20Act,%201992.pdf

Government of India, National Crime Records Bureau, *"About CCTNS"*, http://ncrb.nic.in/AboutCCTNS.htm

Government of India, Ministry of Communication and IT, Department of Telecommunications, *Public Notice*, http://www.dot.gov.in/sites/default/files/sw_30.12.2010_0.pdf

Government of India, Ministry of Communications and Information Technology, Department of Telecommunications, *Licensing*, http://www.dot.gov.in/licensing

Government of India, Ministry of Communications and Information Technology, Department of Telecommunications, *Indian Telegraph Act, 1885*, http://www.ijlt.in/pdffiles/Indian-Telegraph-Act-1885.pdf

Government of India, Ministry of Communications and Information Technology, Department of Telecommunications, *Indian Post Office Act, 1898*, http://www.indiapost.gov.in/Pdf/Manuals/TheIndianPostOfficeAct1898.pdf

Government of India, Ministry of Communications and Information Technology, Department of Telecommunications, *The Indian Wireless Telegraphy Act, 1933*, http://tdsat.nic.in/New%20Compendium19.11.2008/TD%20Set%20Vol-1%20PDF/53-58.pdf

Government of India, National Integration Council (NIA), *The Unlawful Activities (Prevention) Act, 1967*, http://www.nia.gov.in/acts/TheUnlawfulActivities_%28Prevention%29_AmendmentAct,1967%2837of1967%29.pdf

Government of India, Ministry of Communications and Information Technology, *The Code of Criminal Procedure, 1973, Section 91*, http://www.icf.indianrailways.gov.in/uploads/files/CrPC.pdf

Government of India, Ministry of Communications and Information Technology, Department of Telecommunications, *License Agreement for Provision of Basic Telephone Service, 1992*, http://www.usof.gov.in/usof-cms/tender/usotender18Jan07/BasicServiceLicence.pdf

Government of India, Ministry of Communications and Information Technology, Department of Telecomunications, *License Agreement for Provision of Cellular Mobile Telephone Service, 1994*, http://www.usof.gov.in/usof-cms/tender/cmtsAGREEMENT.pdf

Government of India, Ministry of Communications and Information Technology, Department of Telecommunications, *License Agreement for Provision of Internet Services, 1998*, http://www.dot.gov.in/data-services/internet-services

Government of India, Ministry of Communciations and Information Tehcnology, Department of Telecommunications, *License Agreement for Provision of Unified Access Services After Migration from CMTS, 2003*, http://www.dot.gov.in/access-services/unified-access-services

Government of India, Ministry of Communications and Information Technology, Department of Telecommunications, *The Indian Telegraph (Amendment) Rules, 2007*, http://www.dot.gov.in/sites/default/files/march2007.pdf

Government of India, Ministry of Communications and Information Technology, Department of Telecommunications, *"Pertaining to ISP License granted subsequent to guidelines dated 24.08.07"*, http://www.dot.gov.in/data-services/pertaining-isp-licence-granted-subsequent-guidelines-dated-240807

Government of India, Ministry of Communications and Information Technology, Department of Telecommunications, *The Information Technology (Amendment) Act, 2008*, http://police.pondicherry.gov.in/Information%20Technology%20Act%202000%20-%202008%20%28amendment%29.pdf

Government of India, Press Information Bureau, Cabinet Committee on Economic Affairs, *"Crime and Criminal Tracking Network & Systems (CCTNS) project"*, 2009, http://pib.nic.in/newsite/erelease.aspx?relid=49261

Government of India, Ministry of Communications and Information Technology, Department of Information Technology, *"Notification of Rules under Sections 52, 54, 69, 69A, 69B"*, 27th October 2009, http://deity.gov.in/sites/upload_files/dit/files/downloads/itact2000/Itrules301009.pdf

Government of India, Ministry of Home Affairs, Press Information Bureau, *"Home Minister proposes radical restructuring of security architecture"*, 23 December 2009, http://www.pib.nic.in/newsite/erelease.aspx?relid=56395

Government of India, Ministry of Communications and Information Technology, Department of Information Technology, *"The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011"*, 11th April 2011, http://deity.gov.in/sites/upload_files/dit/files/GSR313E_10511%281%29.pdf

Government of India, Ministry of Home Affairs, *National Intelligence Grid*, 30 May 2013, http://www.davp.nic.in/WriteReadData/ADS/eng_19138_1_1314b.pdf

Government of India, Ministry of Communications and IT, Department of Telecommunications, *"Amendment to the UAS License Agreement regarding Central Monitoring System"*, June 2013, http://cis-india.org/internet-governance/blog/uas-license-agreement-amendment

Government of India, Ministry of Communciations and Information Technology, Department of Telecommunications, *License Agreement for Unified License (Access Services), 2013*, http://www.dot.gov.in/sites/default/files/DOC270613-013.pdf

International Organisation for Standardization (ISO), *About ISO*, http://www.iso.org/iso/home/about.htm

International Organisation for Standardization (ISO), *Standards: ISO/IEC 27001 – Information security management"*, http://www.iso.org/iso/home/standards/management-standards/iso27001.htm

International Organisation for Standardization (ISO), *Standards: ISO 9000 – Quality management*, http://www.iso.org/iso/home/standards/management-standards/iso_9000.htm

International Organisation for Standardization (ISO), *"Quality Management Principles"*, 2012, http://www.iso.org/iso/qmp_2012.pdf

Jadine Lannon, *"Information Technology (Procedure and Saefguards for Monitoring and Collecting Traffic Data or Information) Rules, 2009"*, Centre for Internet and Society, 25 April 2013, http://cis-india.org/internet-governance/resources/it-procedure-and-safeguard-for-monitoring-and-collecting-traffic-data-or-information-rules-2009

Jadine Lannon, *"Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009"*, Centre for Internet and Society, 06 July 2013, http://cis-india.org/internet-governance/resources/it-procedure-and-safeguards-for-interception-monitoring-and-decryption-of-information-rules-2009

Jadine Lannon, *"Rule 419A of the Indian Telegraph Rules, 1951"*, Centre for Internet and Society, 19 November 2013, http://cis-india.org/internet-governance/resources/rule-419-a-indian-telegraph-rules-1951

Justice Ajit Prakash Shah, Former Chief Justice, High Court of Delhi, *"Report of the Group of Experts on Privacy"*, Planning Commission (CIT&I Division), Government of India, 16 October 2012, http://planningcommission.nic.in/reports/genrep/rep_privacy.pdf

Kommlabs Dezign, *Events*, http://www.kommlabs.com/events.asp

Kommlabs Dezign, *Solutions for Intelligence Agencies*, http://www.kommlabs.com/solutions-intelligence.asp

Krishna Bahirwani, *"C-DOT's surveillance system making enemies on Internet"*, DNA India, 21 March 2014, http://www.dnaindia.com/mumbai/report-c-dot-s-surveillance-system-making-enemies-on-internet-1970936

Lucian Constantin, *"Developer-signed Mac spyware found on Angolan activist's computer"*, Macworld, 17 May 2013, http://www.macworld.com/article/2038960/developer-signed-mac-spyware-found-on-angolan-activists-computer.html

Margaret Rouse, *"Data Analytics (DA)"*, Tech Target, Data Management, 10 January 2008, http://searchdatamanagement.techtarget.com/definition/data-analytics

Maria Xynou, *"India's 'Big Brother': The Central Monitoring System (CMS)"*, The Centre for Internet and Society (CIS), 08 April 2013, http://cis-india.org/internet-governance/blog/indias-big-brother-the-central-monitoring-system

Maria Xynou, *"The Surveillance Industry in India: At Least 76 Companies Aiding Our Watchers!"*, The Centre for Internet and Society, 02 May 2013, http://cis-india.org/internet-governance/blog/the-surveillance-industry-in-india-at-least-76-companies-aiding-our-watchers

Maria Xynou, *"The India Privacy Monitor Map"*, The Centre for Internet and Society, 09 October 2013, http://cis-india.org/internet-governance/blog/india-privacy-monitor-map

Maria Xynou, *"Spy Files 3: WikiLeaks Sheds More Light On the Global Surveillance Industry"*, The Centre for Internet and Society, 25 October 2013, http://cis-india.org/internet-governance/blog/spy-files-three

Maria Xynou, *"India's Central Monitoring System (CMS): Something to Worry About?"*, Centre for Internet and Society (CIS), 30 January 2014, http://cis-india.org/internet-governance/blog/india-central-monitoring-system-something-to-worry-about

Maria Xynou, *"Big democracy, big surveillance: India's surveillance state"*, OpenDemocracy, 10 February 2014, http://www.opendemocracy.net/opensecurity/maria-xynou/big-democracy-big-surveillance-indias-surveillance-state

Maria Xynou, *Spreadsheet data on sample of 50 security companies*, Centre for Internet and Society, 28 February 2014, http://cis-india.org/internet-governance/blog/data-on-surveillance-technology-companies

Morgan Marquis-Boire, Bill Marczak, Claudio Guarnieri & John Scott-Railton, *"For Their Eyes Only: The Commercialization of Digital Spying"*, The Citizen Lab, 30 April 2013, https://citizenlab.org/2013/04/for-their-eyes-only-2/

Nick Hopkins & Matthew Taylor, *"Private firms selling mass surveillance systems around world, documents show"*, The Guardian, 18 November 2013, http://www.theguardian.com/world/2013/nov/18/private-firms-mass-surveillance-technologies

NT Balanarayan, *"NATGRID Partial Roll Out Very Soon"*, Medianama, 17 January 2014, http://www.medianama.com/2014/01/223-natgrid-partial-roll-out/

Paladion Networks, *Client List*, http://www.paladion.net/client_list.html

Pranesh Prakash, *"How Surveillance Works in India"*, The New York Times, 10 July 2013, http://india.blogs.nytimes.com/2013/07/10/how-surveillance-works-in-india/?_php=true&_type=blogs&_r=0

Prasad Krishna, *"Sixth Meeting of the two Sub-Groups on Privacy Issues under the Chairmanship*

of Justice AP Shah", The Centre for Internet and Society, 23 August 2012, http://cis-india.org/news/sixth-meeting-of-sub-groups-on-privacy-issues

Press Trust of India, *"NATGRID to use Big Data & analytics to track suspects"*, The Business Standard, 29 December 2013, http://www.business-standard.com/article/current-affairs/natgrid-to-use-big-data-analytics-to-track-suspects-113122900191_1.html

Privacy International, *Big Brother Incorporated Project*, https://www.privacyinternational.org/projects/big-brother-inc

Privacy International, Report: *"India"*, Chapter 3: "Surveillance Policies", https://www.privacyinternational.org/reports/india/iii-surveillance-policies

PTI, *"Indian government to launch internet spy system 'Netra' soon"*, DNA India, 05 January 2014, http://www.dnaindia.com/scitech/report-indian-government-to-launch-internet-spy-system-netra-soon-1945867

PTI, *"India to deploy Internet spy system 'Netra'"*, Livemint & The Wall Street Journal, 06 January 2014, http://www.livemint.com/Politics/To4wvOZX7RmLM4VqtBshCM/India-to-deploy-Internet-spy-system-Netra.html

PTI, *"Govt to launch internet spy system 'Netra' soon"*, The Times of India, 06 January 2014, http://articles.timesofindia.indiatimes.com/2014-01-06/internet/45917976_1_security-agencies-netra-cabinet-secretariat

Ray Horak, *Telecommunications and Data Communications Handbook*, Wiley, 21 July 2008

R Ananthapur, "India's new Data Protection Legislation", (2011) 8:2 *SCRIPTed* 192, http://www.law.ed.ac.uk/ahrc/script-ed/vol8-2/ananthapur.asp

Rajiv Nayan, *"Update on India's Membership of Multilateral Export Control Regimes"*, Institute for Defense Studies and Analyses, 19 December 2012, http://idsa.in/idsacomments/UpdateonIndiasMembershipofMultilateralExportControlsRegimes_rnayan_191212

Reserve Bank of India, *Internet Banking in India – Guidelines*, http://www.rbi.org.in/scripts/NotificationUser.aspx?Id=414&Mode=0

Richard Stallman, *"How Much Surveillance Can Democracy Withstand?"*, Wired, 14 October 2013, http://www.wired.com/opinion/2013/10/a-necessary-evil-what-it-takes-for-democracy-to-survive-surveillance/

Ritu Sarin, *"Govt sets norms for lawful interception and monitoring"*, The Indian Express, 17 February 2012, http://archive.indianexpress.com/news/govt-sets-norms-for-lawful-interception-and-monitoring/913034/0

Ritu Sarin, *"States begin to surrender off-the-air phone snooping equipment"*, The Financial Express, 05 June 2012, http://www.financialexpress.com/news/states-begin-to-surrender-offair-phone-snooping-equipment/957859

Ritu Sarin, *"State govts hand over few off-air phone-tapping sets to Centre"*, The Indian Express, 21 October 2013, http://m.indianexpress.com/news/state-govts-hand-over-few-offair-

phonetapping-sets-to-centre/1185166/

Sabir Shah, *"Major terror attacks in India during last 25 years"*, The International News, 28 October 2013, http://www.thenews.com.pk/Todays-News-2-210676-Major-terror-attacks-in-India-during-last-25-years

SECURUS Strategic Trade Solutions, *"India's Export Controls: Current Status and Possible Changes on the Horizon"*, 10 July 2011, http://www.securustrade.com/India%27s%20Export%20Controls_Article__July_10_2011_FINAL.pdf

Sh. P Chidambaram, Ex-Union Home Minister, *"Ex-Union Home Minister's mission statement for NCRB under CCTNS"*, Crime and Criminal Tracking Network & System (CCTNS), National Crime Records Bureau, Ministry of Home Affairs, http://ncrb.nic.in/cctns.htm

Shalini Singh, *"Govt. Violates Privacy Safeguards to Secretly Monitor Internet Traffic"*, The Hindu, 08 September 2013, http://www.thehindu.com/news/national/govt-violates-privacy-safeguards-to-secretly-monitor-internet-traffic/article5107682.ece

SiliconIndia, *"Cloud Computing: A Powerful Tool for Cyber Attacks?"*, SiliconIndia News, 22 January 2014, http://www.siliconindia.com/news/technology/Cloud-Computing-A-Powerful-Tool-For-Cyber-Attacks-nid-159930-cid-2.html

Smitha Krishna Prasad, *"Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009"*, Centre for Internet and Society, 21 November 2013, http://cis-india.org/internet-governance/resources/information-technology-procedure-and-safeguards-for-blocking-for-access-of-information-by-public-rules-2009

Sophie Curtis, *"Privacy International threatens legal action over surveillance tech exports"*, TechWorld, 25 July 2012, http://news.techworld.com/security/3372104/privacy-international-threatens-legal-action-over-surveillance-tech-exports/

Standing Committee on Information Technology (2013-2014), *"Fifty-second Report on Cyber Crime, Cyber Security, and Right to Privacy"*, Ministry of Communications and Information Technology, Department of Electronics and Information Technology, Government of India, Fiftenth Lok Sabha, New Delhi, 12 February 2014, http://164.100.47.134/lsscommittee/Information%20Technology/15_Information_Technology_52.pdf

Subsention: To Notice Secretly, *CALEA "Safe Harbor" in four easy steps*, 22 October 2013, http://www.subsentio.com/live/regulatory/joels-blog-time/safe-harbor-review-20131022/

Sunil Thapliyal, *"Cyber cafe rules too strict?"*, The Hindustan Times, 26 June 2011, http://www.hindustantimes.com/india-news/cyber-cafe-rules-too-strict/article1-713868.aspx

The Hindu, *"Govt launches crime tracking pilot project"*, 04 January 2013, http://www.thehindu.com/news/national/govt-launches-crime-tracking-pilot-project/article4272857.ece

Theresa Krause, *"Data Mining in the Information Age"*, University of Utah, November 2011, http://www.law.utah.edu/wp-content/uploads/Data-Mining-in-the-Information-Age-Krause.pdf

The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies and Munitions List, WA-LIST (13) 1, 04 December 2013, http://www.wassenaar.org/controllists/2013/WA-LIST%20%2813%29%201/WA-LIST%20%2813%29%201.pdf

Vehere, *vCrimes,* http://www.veheretech.com/products/vcrimes/

Verint Systems, *Star-Gate,* http://www.verint.com/solutions/communications-cyber-intelligence/products/star-gate/index

Verint Systems, *Vantage,* http://www.verint.com/solutions/communications-cyber-intelligence/products/vantage/index

Vikas SN, *"Indian Government Plans Internet Monitoring System Netra",* Medianama, 06 January 2014, http://www.medianama.com/2014/01/223-indian-govt-internet-monitoring-system-netra/

V.K. Srivastava & Arvind Madhavan, *"India's Export Control System: Inter-Agency Cooperation and Coordination",* 20th Asian Export Control Seminar, Tokyo, 2012, http://www.simul-conf.com/outreach/2012/asian_ec/2-C2%20Mr%20Madhavan%20&%20Mr%20Srivastava%20%28India%29.pdf

We are Social, *India,* 2014 Edition, http://wearesocial.net/tag/india/

Yatish Yadav, *"New Guidelines Formulated for Monitoring, Interception of Phone Calls",* The New Indian Express, 11 January 2014, http://www.newindianexpress.com/nation/New-Guidelines-Formulated-for-Monitoring-Interception-of-Phone-Calls/2014/01/11/article1994336.ece#.Uw6GUZh_W8Y