Research

Surveillance, Interception and Evidence Gathering:
Local Law and International Precedents

1. Local Law on Surveillance, Interception and Evidence Gathering

A. The Investigation for Fair Trial Act, 2013[1]

The Investigation for Fair Trial Act (IFTA), 2013, requires that a notified officer make an application under the Act, if there is reason to believe that a person may be associated with or is likely to act in a manner that constitutes a scheduled offence. However, the officer is required to obtain a warrant from court for surveillance or interception.

Prior to obtaining a warrant, the applicant is required to prepare a report with supporting material, present it to the Minister (Federal Minister for Interior) for permission and then move the application before a judge for issuance of the warrant. A warrant under the Act is to be issued by a judge of the High Court in chamber. Section 8 of IFTA 2013 lists the requirements the applicant must meet when seeking permission for surveillance or interception, whereas Section 10 pertains to what is to be considered by the judge when issuing a warrant. The duration of the warrant under Section of the Act is 60 days. It may be re-issued for another 60 days after a fresh application is made and reasons presented by the applicant, for why the earlier time period was insufficient

If the request by the applicant is deemed arbitrary by the judge, under Section 15 of the law, departmental action can be recommended against the officer. Under Section 22 of the Act, the authorised officer is required to certify the evidence collected is strictly in accordance with the warrant and has not been tampered with or altered, before turning it over to the investigating officer.

How many – if any – warrants have been obtained under the Investigation for Fair Trial Act, 2013, prior to conducting surveillance or intercepting communications of individuals?

[1] http://www.na.gov.pk/uploads/documents/1361943916_947.pdf

B. The Prevention of Electronic Crimes Act, 2016[2]

The Prevention of Electronic Crimes Act (PECA), 2016, criminalises “unauthorised access to information system or data,” “unauthorised copying or transmission of data,” “interference with information system or data,” “unauthorised use of identity information” and “unauthorised interception.”

The Federal Investigation Agency (FIA) was designated as the investigation agency under PECA 2016 by the Federal Cabinet, in accordance with Section 29 of the Act. Only an authorised officer of the investigation agency can exercise powers under the PECA 2016 and must follow the procedures laid down in the Act and the Prevention of Electronic Crimes Investigation Rules, 2018[3]. Powers of an authorised officer are outlined in Section 35 of the Act.

Section 32 of PECA 2016 requires service providers to retain traffic data for a period of one year. This data can only be provided to the investigation agency subject to a warrant issued by the court. Section 33 of the Act requires an authorised officer to make an application before the court, obtain a warrant and then conduct search and seizure, that too, of the specified place.

The only exception is if the offence falls under Section 10 of the Act and there is reason to believe there could be destruction or alteration of data, in which case the authorised officer may proceed to conduct search and seizure without a warrant, but still of a specified premises. The officer must bring this to the knowledge of the court within twenty-four hours.

Section 34 of the Act requires an authorized officer to obtain a warrant in order to gain access to content data stored in an information system. Section 36 of the Act outlines how seized data or information systems are supposed to be dealt with. Rule 8 of the PECA Investigation Rules, 2018, requires that a proper chain of custody be maintained when devices are seized so that the integrity, security and proper documentation of seized items is maintained.

---

[2] http://www.na.gov.pk/uploads/documents/1472635250_246.pdf

[3] http://bolobhi.org/wp-content/uploads/2019/01/PECA-RULES.pdf

Section 39 pertains to the “real-time collection and recording of information.” An authorised officer is required to seek the court’s permission prior to carrying out this function. Collection and recording of information has to be in connection to a criminal investigation, for a period of seven days. An extension beyond seven days is only allowed after seeking the court’s permission. Section 42 of the Act requires the Federal Government to designate or set up a forensic lab independent of the investigation agency.

How many – if any – warrants have been obtained under the Prevention of Electronic Crimes Act, 2016, prior to conducting search and seizure, obtaining traffic and content data or real-time collection and recording of information?

C. Scenarios and Concerns:

While the law subjects surveillance, interception and the recording and collection of data to warrants, judicial oversight and some procedural checks, how much is actually followed in practice? Over the years there have been reports issued by international organizations[4], which point to the deployment of surveillance tech in Pakistan. Such technology enables a blanket and continuous surveillance regime without any oversight. Invasive tech tools mean the ability to go beyond the legally permissible duration and methods of surveillance and interception, under both IFTA, 2013 and PECA 2016, in contravention of mandatory provisions of the law.

In carrying out surveillance and interception in this manner[5], more than just the alleged offender comes under scrutiny. By default, all those who communicate with the person being surveilled, are intercepted and become subjects of surveillance. Private conversations, data, images are sometimes misused to blackmail and intimidate individuals. Roving inquiries and phishing expeditions are conducted to extract information then construct cases against them versus having reasonable grounds to do so in the first place[6].

Irregularities[7], lack of independent, third-party verification for IP traces and forensics reports raise issues of veracity and credibility of claims regarding the evidence submitted. There exist no mechanisms to independently ascertain whether the chain of custody, integrity and security of a device was maintained, how to detect tampering if it happened or if material was planted and then forensics conducted.

[4] https://bolobhi.org/resources-on-filtering-and-surveillance-in-pakistan/
[5] https://bolobhi.org/internet-surveillance/
[6] http://bolobhi.org/timeline-summons-enquiries-firs-detentions-and-arrests-in-connection-with-social-media-posts-2/
[7] https://bolobhi.org/wp-content/uploads/2019/11/Summary-of-Report-updated-18.10.2019.pdf

2. International Obligations and Global Principles on Communications Surveillance and Privacy

A. International Covenant on Civil and Political Rights

Article 17

1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.

2. Everyone has the right to the protection of the law against such interference or attacks.

B. 13 principles on communications surveillance - EFF and a coalition of NGOs

1. Legality
2. Legitimate Aim
3. Necessity
4. Adequacy
5. Proportionality
6. Competent Judicial Authority
7. Due Process
8. User Notification
9. Transparency
10. Public Oversight
11. Integrity of Communications and Systems
12. Safeguards for International Co-operation
13. Safeguards Against Illegitimate Access and Right to Effective Remedy

C. The GNI Principles

"Privacy is a human right and guarantor of human dignity. Privacy is important to maintaining personal security, protecting identity and promoting freedom of expression in the digital age.

Everyone should be free from illegal or arbitrary interference with the right to privacy and should have the right to the protection of the law against such interference or attacks.[xi]

The right to privacy should not be restricted by governments, except in narrowly defined circumstances based on internationally recognized laws and standards. These restrictions should be consistent with international human rights laws or standards, the rule of law and be necessary and proportionate for the relevant purpose.

- Participating companies will employ protections with respect to personal information in all countries where they operate in order to work to protect the privacy rights of users.
- Participating companies will respect and work to protect the privacy rights of users when confronted with government demands, laws or regulations that compromise privacy in a manner inconsistent with internationally recognized laws and standards."

3. International Reports, Articles, Case Studies and Case Law on Surveillance, Sting Operations and Evidence Gathering

Year	Reports	News Articles/ Case Studies/ Press Releases
2020	1. New Report on "The Use of Biometric Data to Identify Terrorists: Best 1. New report by the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Prof. Fionnuala Ní Aoláin and Dr. Krisztina Huszti-Orbán on the "Use of Biometric Data to Identify Terrorists: Best Practice or Risky Business?". 2. The report explores the human rights risks involved in the deployment of biometrics in counter-terrorism context. 3. PI previously highlighted concerns about the obligations imposed on UN Member States by Resolution 2396 use of biometric data in counter-terrorism which echo the recommendations presented in this report.	1. Fuelled by Leaked Evidence and Illegal Surveillance, Media Trials the New Normal in India "Pro-government media channels and platforms are now directly obtaining classified evidence from investigating agencies and the police, a thoroughly illegal act." 2. FISA Court Opinion Outlines FBI Abuse of Key Intelligence Surveillance Authority "The Court charged with overseeing US surveillance authorities has rendered a bombshell ruling: the Federal Bureau of Investigation is using authorities aimed at surveilling foreigners abroad to investigate Americans impermissibly. Instead of using Section 702 of the Foreign Intelligence Surveillance Act (FISA) to prevent foreign terrorist

	4. A human rights approach is imperative to ensure an effective counter-terrorism strategy and below we highlight what a human rights approach should at least involve. 2. We Chat, They Watch - How International Users Unwittingly Build up WeChat's Chinese Censorship Apparatus ● "We present results from technical experiments which reveal that WeChat communications conducted entirely among non-China-registered accounts are subject to pervasive content surveillance that was previously thought to be exclusively reserved for China-registered accounts. ● Documents and images transmitted entirely among non-China-registered accounts undergo content surveillance wherein these files are analyzed for content that is politically sensitive in China. ● Upon analysis, files deemed politically sensitive are used to invisibly train and build	attacks and collect foreign intelligence, it used information collected under this program to vet Americans who wanted to become police officers, to vet American college students participating in a "Collegiate Academy," and to check out Americans who had visited an FBI office. In one stunning disclosure, the Foreign Intelligence Surveillance Court (FISA Court) found that the FBI used the identifiers of 16,000 Americans to comb through the data collected under this program, even though the FBI could legally justify only seven of those 16,000 queries based on the required foreign intelligence or crime-fighting purposes." 3. CDT Joins OTI in Amici Brief in Wikimedia V. NSA "This case raises an important question: Whether the U.S. government's Upstream surveillance under Section 702 of the Foreign Intelligence Surveillance Act ("FISA"), involving the bulk interception of Internet communications, is lawful and constitutional." 4. Why we're taking the UK government to court over mass spying

	up WeChat's Chinese political censorship system. ● From public information, it is unclear how Tencent uses non-Chinese-registered users' data to enable content blocking or which policy rationale permits the sharing of data used for blocking between international and China regions of WeChat. ● Tencent's responses to data access requests failed to clarify how data from international users is used to enable political censorship of the platform in China." 3. WeChat Surveillance Explained 1. WeChat surveils non-China-registered accounts and uses messages from those accounts to train censorship algorithms to be used against China-registered accounts. 2. Both the monitoring and censorship happen in secret, without transparency to users. 3. None of WeChat's public-facing policy documents, personal data access requests processes, or privacy officers communicated	"GCHQ's Tempora programme works by intercepting data in most of the fibre-optic communications cables in and out of the country. Because a large proportion of everyone's daily communications – for example, emails on Gmail, Yahoo Mail or Outlook.com, or Facebook messages – involve US companies, it is very likely the data will travel through servers outside the UK. 36 million people in the UK use Facebook. Through our social media use alone, GCHQ can keep tabs on more than half the UK's population." 5. German court limits power of spy agency's overseas bugging Germany's Constitutional Court has ruled that the surveillance of telephones and internet traffic of foreign nationals abroad by the BND intelligence agency violates parts of the constitution, a victory for overseas journalists who brought the case. 6. Two iPhones or the privacy of billions: Why Apple vs. the FBI matters

	that the company is conducting this surveillance.	The FBI has likewise been grilled on its own credibility. An inspector general report from 2018 said that the FBI headed to court against Apple in the San Bernardino dispute without first exhausting its technical options. And the FBI acknowledged to The Washington Post that it had repeatedly inflated the number of devices it couldn't access. 7. The FBI and Apple are facing off over an iPhone again. What's going on? "the US attorney general, William Barr, called on Apple to help the Federal Bureau of Investigation (FBI) unlock two iPhones related to the fatal shooting of three Americans at a Florida naval base in December. The shooting, by a Saudi air force cadet who was training with US forces, is now considered an act of terrorism, Barr said."
2019	**1.** Privacy International's submission to the UN Human Rights Committee on Article 21 of the ICCPR	4. A Declassified Court Ruling Shows How the FBI Abused NSA Mass Surveillance Data "Among the abuses noted in the ruling:

	"In this submission, Privacy International aims to provide the Committee with information on how surveillance technologies are affecting the right to peaceful assembly in new and often unregulated ways. Based on Privacy International's research, we provide the following observations: 1. the relationship between right to peaceful assembly and right to privacy; 2. right to peaceful assembly and new surveillance technologies; 3. right to peaceful assembly online." 2. Not A Secret: Bulk Interception Practices of Intelligence Agencies "In setting out how transparent other countries are able to be in both the law governing bulk cable collection and the technical practice, this report seeks to counter the assertion that similar levels of transparency in the U.S. would amount to a grave risk to U.S. national security. Excessive secrecy is thwarting public debate about whether to permit bulk cable interception at all, and whether efforts to	• During a four-day period in March 2017, the FBI searched mass surveillance data for communications related to an FBI facility, suggesting that agents were spying on other agents. • On one day alone, on December 1, 2017, the FBI conducted 6,800 queries using Social Security numbers. • A contract linguist for the FBI conducted searches on himself, other FBI employees, and relatives. • The FBI regularly used mass surveillance data to investigate potential witnesses and informants who were neither suspected of crimes nor national security concerns."

	outlaw the practice of bulk collection domestically have been effective." 3. Social Media Surveillance "Governments are increasingly purchasing sophisticated technology to monitor their citizens' behavior on social media. Once the preserve of the world's foremost intelligence agencies, this form of mass surveillance has made its way to a range of countries, from major authoritarian powers to smaller or poorer states that nevertheless hope to track dissidents and persecuted minorities. The booming commercial market for social media surveillance has lowered the cost of entry not only for the security services of dictatorships, but also for national and local law enforcement agencies in democracies, where it is being used with little oversight or accountability. Coupled with an alarming rise in the number of countries where social media users have been arrested for their legitimate online activities, the growing employment of social media surveillance threatens to squeeze the space for civic activism on digital platforms."	

2018	1. Canada: Annual Report on the Use of Electronic Surveillance - 2018 "Part VI of the *Criminal Code* sets out the provisions for the law enforcement community to obtain judicial authorization to conduct electronic surveillance of private communications for criminal investigations. This section also sets out provisions to conduct electronic surveillance of private communications without judicial authorization when there is imminent harm, such as in the case of kidnappings or bomb threats. These procedures are to be carried out in such a way so as to ensure that the privacy of individuals is respected as much as possible during the surveillance. As a measure of accountability, section 195 of the *Criminal Code* requires the Minister of Public Safety and Emergency Preparedness to prepare and present to Parliament an annual report on the use of electronic surveillance under Part VI for offences that may be prosecuted by, or on behalf of, the Attorney General of Canada.	1. GCHQ data collection regime violated human rights, court rules "GCHQ's methods for bulk interception of online communications violated privacy and failed to provide sufficient surveillance safeguards, the European court of human rights has ruled. But the ECHR found that GCHQ's regime for sharing sensitive digital intelligence with foreign governments was not illegal, and it explicitly confirmed that bulk interception with tighter safeguards was permissible. The ruling, which follows Edward Snowden's whistleblowing revelations, is a comprehensive assessment by the ECHR of interception operations carried out until recently by UK intelligence agencies." 2. Fighting Mass Surveillance in the Post-Snowden Era "The Snowden revelations irrevocably changed the public's understanding of the scope and scale of

	The 2018 Annual Report covers a five-year period from 2014 to 2018. The Report includes new statistics for the period from January 1, 2018 to December 31, 2018 and updated figures for the years 2014 to 2017." 15	surveillance undertaken by intelligence agencies. As methods of communications have changed, surveillance techniques have also evolved to permit the collection, storage, analysis and dissemination of personal information at population-scale. We now know that the NSA recorded every single mobile phone call into, out of, and within at least two countries; it collected hundreds of millions of contact lists and address books from personal email and instant-messaging accounts; and surreptitiously intercepted data from Google and Yahoo user accounts as that information travelled between those companies' data centres located abroad. We also know that both the NSA and GCHQ conduct mass interception of internet traffic transiting undersea fiber-optic cables; that GCHQ conducts mass hacking both domestically and abroad; and that the US, UK (and the rest of the Five Eyes alliance) have broad access to information gathered through each country's respective surveillance programs." 3. What a European Court Ruling Means for Mass Spying Around the World (Article)

		"Following a lawsuit initiated by Privacy International and nine other CSOs, the European Court of Human Rights (ECtHR) ruled that the UK government's mass interception program violates the rights to privacy and freedom of expression because of insufficient safeguards and lack of oversight. That decision laid the groundwork for influencing the UK government to adjust current legislation and practices in compliance with the Court's findings, although the changes are on hold as the Grand Chamber of the ECtHR is now considering the case."
2017	1. Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU – by the EU Agency for fundamental rights: "Digital surveillance methods serve as important resources in intelligence efforts, ranging from intercepting communications and metadata to hacking and database mining. But – as the 2013 Snowden revelations underscored – these activities may also seriously interfere with diverse	1. NSA Secretly Helped Convict Defendants in U.S. Courts, Classified Documents Reveal "Kurbanov does not appear to be the only defendant kept in the dark about how warrantless surveillance was used against him. A nationwide review of federal court records by The Intercept found that of 75 terrorism defendants notified of some type of FISA spying since Section 702 became law, just 10 received notice of Section 702 surveillance. And yet Section 702 was credited with "well over 100 arrests on terrorism-related offenses" in a July 2014 report from the Privacy and Civil

	fundamental rights, particularly to privacy and data protection. This report constitutes the second part of a research effort triggered by a European Parliament request for in-depth research on the impact of surveillance on fundamental rights. It updates FRA's 2015 legal analysis (Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU – Volume I: Member States' legal frameworks). In addition, it presents findings from over 70 interviews with experts – conducted largely in 2016 – in seven EU Member States: Belgium, France, Germany, Italy, the Netherlands, Sweden and the United Kingdom. The report focuses on large-scale technical collection of intelligence, referred to as general surveillance of communications." 2. Reckless Exploit - Mexican Journalists, Lawyers, and a Child Targeted with NSO Spyware	Liberties Oversight Board, the federal entity created to oversee intelligence authorities granted in the wake of the 9/11 attacks. Additional documents from Snowden, previously unpublished and dated before the Kurbanov case, provide further examples of how NSA intelligence repeatedly played an undisclosed role in bringing accused terrorists to trial in U.S. courts over the past decade and a half. They also reveal an instance in which the NSA incorrectly identified a U.S. citizen as a foreign target of a FISA warrant." 2. There's No Good Reason for Spy Agencies to Snoop on Humanitarian Groups "In one of the least-discussed stories arising out of the materials leaked by Edward Snowden, in December 2013 the Guardian reported that the NSA and GCHQ, a British intelligence agency, are targeting humanitarian agencies such as UNICEF, the U.N. Development Program, and Medecins du Monde (Doctors of the World). Each of those organizations, named in leaked GCHQ documents, had been allocated a specific ID number in GCHQ's "target knowledge base," indicating they had been identified for targeted surveillance by the agency. The United Nations made no public response to the allegations. When Medecins du Monde wrote to GCHQ seeking an explanation, the intelligence service

	1. Over 76 messages with links to NSO Group's exploit framework were sent to Mexican journalists, lawyers, and a minor child (NSO Group is a self-described "cyber warfare" company that sells government-exclusive spyware). 2. The targets were working on a range of issues that include investigations of corruption by the Mexican President, and the participation of Mexico's Federal authorities in human rights abuses. 3. Some of the messages impersonated the Embassy of the United States of America to Mexico, others masqueraded as emergency AMBER Alerts about abducted children. 4. At least one target, the minor child of a target, was sent infection attempts, including a communication impersonating the United States Government, while physically located in the United States.	refused to answer any questions. The Guardian says that the documents 'do not disclose the extent of any surveillance or for how long any collection took place.' Yet given what we know about the NSA and GCHQ, it seems likely that the surveillance continues, and that it involves gathering data held in humanitarian databases and intercepting groups' calls, e-mails and text messages. The vast array of issues addressed and programs run by humanitarian organizations mean that this could include data on ethnic communities fleeing genocide, women subjected to sexual violence, child soldiers, refugees from conflicts in Syria and Afghanistan, and impoverished areas suffering serious health problems."

2017	3. Commercial Spyware - The Multibillion Dollar Industry Built on an Ethical and Legal Quagmire "Our research, which documents new attacks against civil society by government actors based in and operating from Ethiopia, highlights the need for clear legal pathways for extraterritorially-targeted individuals to seek recourse. At this juncture, the Ethiopian government's penchant for commercial spyware is notorious, as is its pattern of digital espionage against journalists, activists, and other entities—many of which are based overseas—that seek to promote government accountability and are therefore viewed as political threats. Yet the Ethiopian government and others like it have faced little pressure to cease this particular strain of digital targeting." 4.Social Engineering Attacks on Government Opponents: Target Perspectives	

	1. Surveillance of activists, NGOs, and civil society has moved beyond passive methods and towards hacking devices to retrieve information. This is mainly due to the increased use of encryption, as well as a desire to target those beyond a nation-state's borders. 2. This kind of hacking often involves social engineering as a first step to try and get the target to open a malicious artifact like a link or attachment in a message. In some cases, this can involve the use of products or services by commercial lawful interception vendors. 3. Interviewees had similar behaviours to ordinary users but they have different perceptions of risk. More than half of the on-the-ground activists feared that surveillance would lead to government punishment. 4. Interviewees also used specific security behaviours, such as using out-of-country	

	human password managers to maintain the security of online accounts. 5. Interviewees performed basic vetting before opening attachments but their level of checking could still be vulnerable to sender spoofing and doppelganger accounts. This is particularly true if a victim's friend or contact is compromised. 6. Marczak and Paxson suggest that a tool supporting automated message checking could benefit CSOs, activists, and NGOs.	
2016	1. The Global Surveillance Industry 1. Electronic surveillance techniques have been central to law enforcement and intelligence agencies since the Cold War. Privacy International notes how the proliferation of these technologies are partly driven by weak regulatory mechanisms, the low cost of these techniques, and technological developments. 2. This report describes the different types of technologies that fall within the surveillance industry, including data analysis, audio	1. Apple v the FBI - a plain English guide "'Apple chief executive Tim Cook says the FBI's court order to access the mobile phone of San Bernardino killer Syed Farook is "dangerous", "chilling" and "unprecedented'. The FBI says Apple's lack of co-operation is hindering its investigation."

	surveillance, video surveillance, phone monitoring, location monitoring, Internet monitoring, monitoring centres, intrusion equipment, biometrics, counter-surveillance technology, and forensics. 3. The report also describes the regulatory mechanisms and trade controls in place to manage the trade of surveillance technologies. In 2012, phone monitoring technology was added to the Wassenaar Arrangement list and, in 2013, intrusion software and a provision on Internet monitoring technology were also added. 4. The report concludes by saying that safeguards are a matter of urgency in this space and that a comprehensive approach is necessary for incorporating both export restrictions, where possible, and improved standards in corporate social responsibility.	2. Privacy victory! Surveillance of wireless communications declared unconstitutional in France "The French Constitutional Council declared unconstitutional a section of the French Intelligence Law adopted last year that authorised, without meaningful privacy safeguards or oversight, authorities to monitor and control wireless communications. Responsible for this victory for our right to privacy is the Exégètes amateurs, the legal team for La Quadrature du Net, the French Data Network, and FFDN, the Federation of Non-Profit Internet Service Providers."

2016	1. The Million Dollar Dissident - NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender "Ahmed Mansoor is an internationally recognized human rights defender, based in the United Arab Emirates (UAE), and recipient of the Martin Ennals Award (sometimes referred to as a "Nobel Prize for human rights"). On August 10 and 11, 2016, Mansoor received SMS text messages on his iPhone promising "new secrets" about detainees tortured in UAE jails if he clicked on an included link. Instead of clicking, Mansoor sent the messages to Citizen Lab researchers. We recognized the links as belonging to an exploit infrastructure connected to NSO Group, an Israel-based "cyber war" company that sells *Pegasus*, a government-exclusive "lawful intercept" spyware product. NSO Group is reportedly owned by an	1. Do We Have A Pattern Of Police Entrapment In Canada? "Last week, Justice Catherine Bruce, a judge from British Columbia, made history in Canada and in North America in general. She ruled that John Nutall and Amanda Korody, two Canadian convicted on terrorism charges, were instead entrapped by the RCMP. What was called in the media as the Victoria bomb plot, was rather a pure creation of the 240 RCMP agents who were paid in almost one million dollars in overtime money. Both defence lawyers of Nutall and Korody and Justice Bruce named it: 'manufactured crime.'"

	American venture capital firm, Francisco Partners Management. The ensuing investigation, a collaboration between researchers from Citizen Lab and from Lookout Security, determined that the links led to a chain of zero-day exploits ("zero-days") that would have remotely jailbroken Mansoor's stock iPhone 6 and installed sophisticated spyware. We are calling this exploit chain *Trident*. Once infected, Mansoor's phone would have become a digital spy in his pocket, capable of employing his iPhone's camera and microphone to snoop on activity in the vicinity of the device, recording his WhatsApp and Viber calls, logging messages sent in mobile chat apps, and tracking his movements."	

	2. ASSESSING THE LEGALITY AND PROPORTIONALITY OF COMMUNICATIONS SURVEILLANCE IN UNITED STATES LAW (2016) "This report begins an analysis and discussion of U.S. law and surveillance practices, measured against two key principles of the 13 Principles—Legality and Proportionality. Although this paper does not provide exhaustive coverage of all state and federal laws governing communications surveillance in the United States it attempts to identify and discuss significant themes present in U.S. surveillance law."	
2015	1. (2015) Beyond Privacy: Articulating the Broader Harms of Pervasive Mass Surveillance	1. UN must reject mass surveillance to protect global privacy rights "In response to a consultation being undertaken by the UN in accordance with December's General Assembly resolution on the right to privacy in the digital age,

	"This article begins by recounting a series of mass surveillance practices conducted by members of the "Five Eyes" spying alliance. While boundary- and intersubjectivity-based theories of privacy register some of the harms linked to such practices I demonstrate how neither are holistically capable of registering these harms. Given these theories' deficiencies I argue that critiques of signals intelligence surveillance practices can be better grounded on why the practices intrude on basic communicative rights, including those related to privacy. The crux of the argument is that pervasive mass surveillance erodes essential boundaries between public and private spheres by compromising populations' abilities to freely communicate with one another and, in the process, erodes the integrity of democratic processes and institutions. Such erosions are captured as privacy violations but, ultimately, are more destructive to the fabric of society than are registered by theories of privacy alone. After demonstrating the value of adopting a communicative rights approach to critique signals intelligence surveillance I conclude	Privacy International today called on the United Nations to recognise that mass surveillance is incompatible with human rights. The submission to the Office of the High Commissioner to Human Rights confronts some of the biggest challenges to the right to privacy in the digital age, debunks some of the justifications put forth by the Five Eyes governments in response to the Snowden revelations, and argues that States owe human rights obligations to all individuals subject to their jurisdiction. Privacy International - in conjunction with Access, the Electronic Frontier Foundation, Article 19, the Association for Progressive Communications, Human Rights Watch and the World Wide Web Foundation - demand that the UN formally recognises that indiscriminate surveillance, such as the Prism and Tempora programmes being conducted by the NSA and GCHQ, are inherently disproportionate infringements on individual privacy, and can never be compatible with human rights."

	by arguing that this approach also lets us clarify the international normative implications of such surveillance, that it provides a novel way of conceptualizing legal harm linked to the surveillance, and that it showcases the overall value of focusing on the implications of interfering with communications first, and as such interferences constituting privacy violations second. Ultimately, by adopting this Habermasian inspired mode of analysis we can develop more holistic ways of conceptualizing harms associated with signals intelligence practices than are provided by either boundary- or intersubjective-based theories of privacy.	
2015	1. Tipping the Scales: Security and Surveillance in Pakistan	1. Victory! UK Surveillance Tribunal Finds GCHQ-NSA Intelligence Sharing Unlawful "Today's judgement represents a monumental leap forward in efforts to make intelligence agencies such as

	"Through investigation and analysis of the private surveillance industry's role in Pakistan by Privacy International, the report shows that mass network surveillance has been in place in Pakistan since at least 2005. The Pakistani government obtained this technology from both domestic and foreign surveillance companies including Alcatel, Ericsson, Huawei, SS8 and Utimaco. This report reveals for the first time some of the previously unknown surveillance capacities of the Pakistani government. It also finds that the practical capacity of the Pakistani government, particularly the Inter-Services Intelligence Agency, now outstrips the capacity of domestic and international law for effective regulation of that surveillance. This report contains recommendations for how Pakistan might move away from its current surveillance model to one that complies with applicable human rights law standards, and, as such, no longer represents a threat to Pakistani democracy."	GCHQ and NSA accountable to the millions of individuals whose privacy they have violated."
2014	1. Citizen Lab. Communities @ Risk: Targeted Digital Threats Against Civil Society. Citizen	1. Edward Snowden: US government spied on human rights workers

	Lab, University of Toronto, November 11, 2014. While the Internet and digital technologies have brought upon many benefits for human rights defenders (HRDs), they also have many risks. For example, governments have been able to exploit the Internet and other digital technologies as tools of mass surveillance for national security and foreign policy aims. There have also been a growing number of case studies and reports of journalists and HRDs being targeted by governments with malicious software (malware) or commercial spyware. This report provides a detailed overview of the different types of targeted digital threats and the distinct models that characterize the capacities and tactics of such threat actors. Three are considered here: (1) advanced persistent threats (APTs) characterized by threat actors with the capacity to develop their own resources and conduct wide scale operations;	"Whistleblower tells Council of Europe NSA deliberately snooped on groups such as Human Rights Watch and Amnesty International."

	(2) repurposed crimeware (e.g., Remote Access Trojans circulated amongst hobbyists and criminals); and (3) commercial "lawful intercept" products or commercial spyware where private companies offer states turnkey surveillance solutions.	
2011	1. Using Public Surveillance Systems for Crime Control and Prevention: A Practical Guide for Law Enforcement and Their Municipal Partners – By Urban Institute, and U.S. Department of Justice "The purpose of this guidebook is to aid municipalities and law enforcement agencies in making informed decisions on the implementation or expansion of a public surveillance system. It is intended to equip city administrators with details regarding the cost considerations behind camera use and the potential benefits of such a system, and provide guidance on how to yield the greatest possible crime prevention and investigative impact."	1. Wikileaks release shows terrifying power of today's surveillance industry (Press Release) "Devices small enough to be carried in a rucksack or briefcase that masquerade as legitimate mobile phone base stations in order to intercept and decrypt SMS messages and phone calls from all mobile phones within a radius of several hundred metres ('IMSI catchers'). Malware and spyware that gives the purchaser complete control over a target's computer while allowing the interception to remain undetected. Trojans that, once installed in a mobile phone, allow the purchaser to remotely turn on the phone's microphone and camera in order to record sound and take photographs of the phone's location and user.

		'Optical cyber solutions' for mass surveillance of entire populations, involving tapping the submarine cable landing stations that carry all communications traffic in and out of countries. These techniques were originally developed by the NSA in the 1990s, and until now have been a closely guarded secret."
2009	1. Current practice sin electronic surveillance in the investigation of serious and organized crime – By the UNODC "For those jurisdictions without any regulation, or with legislation which is lacking in some respect, the challenge is to develop a balanced system for the use of electronic evidence gathering. The balance which needs to be struck is that between the effective use of electronic evidence gathering and the protection of citizens' rights. This includes balancing the cost of utilizing these methods against the ultimate public benefit gained from a conviction. These considerations should be weighed carefully by legislators, prosecutors, law enforcement and the like."	

2005	1. Sting Operations, Undercover Agents, and Entrapment – By Bruce Hay in the Missouri Law Review "The Article is organized as follows. Part I is a general overview of the nature of sting operations, their purposes, their potential advantages over other enforcement methods, and the dangers they pose. Parts II and III analyze, respectively, the informational and deterrent effects of sting operations. Part IV considers the relation between the informational and deterrent effects, emphasizing the tensions between them. Part V attempts a model of a socially desirable sting operation, balancing its informational and/or deterrent value against the danger of entrapping otherwise-innocent individuals. 6 The model creates a framework for identifying desirable sting operations, a framework that is necessarily very general in character. To apply it to particular cases would require knowledge of parameters whose value is an empirical question the Article does not attempt to quantify. Part VI briefly discusses some general applications to entrapment doctrine. Part VII concludes."	

4. Entrapment, Sting operations and Rights

1. Sorrells v. United States, 287 U.S. 435 (1932)

U.S. Supreme Court

Sorrells v. United States, 287 U.S. 435 (1932)

Sorrells v. United States

No. 177

Argued November 8, 1932

Decided December 19, 1932

287 U.S. 435

Syllabus

1. Where application of a penal statute, according to its literal meaning, would produce results contrary to the plain purpose and policy of the enactment, and flagrantly unjust, another construction should be adopted if possible. P. 287 U. S. 446.

2. The National Prohibition Act, though denouncing generally as criminal the sale of intoxicating liquor for beverage purposes, was

Page 287 U. S. 436

not intended to apply where the sale is instigated by a prohibition agent for the purpose of luring a person, otherwise innocent, to the commission of the crime so that he may be arrested and punished. P. 287 U. S. 448.

3. The defense of entrapment cannot be attributed to any power in the courts to grant immunity or defeat prosecution when a penal statute has been violated; it depends upon the scope of the statute alleged to have been violated -- *i.e.,* whether the statute should be construed as intending to apply in the particular case. P. 287 U. S. 449.

4. That the issue of entrapment will involve collateral inquiries as to the activities of government agents and as to the conduct and purposes of the defendant previous to the alleged offense is not a valid reason for rejecting entrapment as a defense. P. 287 U. S. 451.

5. Entrapment is available as a defense under a plea of not guilty; it need not be set up by a special plea in bar. P. 287 U. S. 452.

6. Evidence of entrapment in this case *held* such that it should have been submitted to the jury. P. 287 U. S. 452.

57 F.2d 973 reversed.

Certiorari to review the affirmance of a sentence for violation of the Prohibition Act. The certiorari was limited to the question whether evidence on the issue of entrapment was sufficient to go to the jury.

Page 287 U. S. 438[8]"

[8] https://supreme.justia.com/cases/federal/us/287/435/

2. Sherman v. United States, 356 U.S. 369 (1958)

U.S. Supreme Court

Sherman v. United States, 356 U.S. 369 (1958)

Sherman v. United States

No. 87

Argued January 16,1958

Decided May 19, 1958

356 U.S. 369

Syllabus

At petitioner's trial in a Federal District Court for selling narcotics in violation of 21 U.S.C. § 174, he relied on the defense of entrapment. From the undisputed testimony of the Government's witnesses, it appeared that a government informer had met petitioner at a doctor's office where both were being treated to cure narcotics addiction, the informer asked petitioner to help him to obtain narcotics for his own use, petitioner seemed reluctant to do so, the informer persisted, and finally petitioner made several small purchases of narcotics and let the informer have half of each amount purchased at cost plus expenses. By prearrangement, other government agents then obtained evidence of three similar sales to the informer, for which petitioner was indicted. Except for a record of two convictions nine and five years previously, there was

no evidence that petitioner himself was in the trade, or that he showed a "ready complaisance" to the informer's request. The factual issue whether the informer had persuaded the otherwise unwilling petitioner to make the sale or whether petitioner was already predisposed to do so and exhibited only the natural hesitancy of one acquainted with the narcotics trade was submitted to the jury, which found petitioner guilty.

Held: on the record in this case, entrapment was established as a matter of law, and petitioner's conviction is reversed. Pp. 356 U. S. 370-378.

(a) Entrapment occurs only when the criminal conduct was "the product of the creative activity" of law enforcement officials. P. 356 U. S. 372.

(b) The undisputed testimony of the Government's witnesses established entrapment as a matter of law. P. 356 U. S. 373.

(c) Although the informer was not being paid, the Government cannot disown him or disclaim responsibility for his actions, since he was an active government informer who was himself awaiting trial on narcotics charges, for which he was later given a suspended sentence. Pp. 356 U. S. 373-374.

Page 356 U. S. 370

(d) It make no difference that the sales for which petitioner as convicted occurred after a series of sales, since they were not independent acts subsequent to the inducement, but were part of a course of conduct which was the product of the inducement. P. 356 U. S. 374.

(e) The Government cannot make such use of an informer and then claim disassociation through ignorance of the way in which he operated. Pp. 356 U. S. 374-375.

(f) The evidence was insufficient to overcome the defense of entrapment by showing that petitioner evinced a "ready complaisance" to accede to the informer's request. Pp. 356 U. S. 375-376.

(g) This Court adheres to the doctrine of the Court's opinion in *Sorrells v. United States,* 287 U. S. 435, and declines to reassess the doctrine of entrapment according to the principles announced in the separate opinion Mr. Justice Roberts in that case, such issues not having been raised by the parties either in this Court or in the lower courts. Pp. 356 U. S. 376-378.

240 F.2d 949 reversed, and cause remanded.[9]"

3. Jacobson v. United States: Do the Ends Justify the Means in Government Stings? (1992) By Maureen Duffy

"During the last few decades, the United States government has been using increasingly elaborate undercover stings to detect and punish criminals. Proponents of stings argue that they are often the only effective means of law enforcement. Some critics contend, however, that these operations infringe on individual rights."

4. The Entrapment Defense: An Interview with Paul Marcus (2004)

[9] https://supreme.justia.com/cases/federal/us/356/369/