State Transgression on Electronic Expression: Is it for Real?

Full Paper

Argha Ray
Tata Consultancy Services
argha.ray@tcs.com

Anjali Kaushik
Management Development Institute
anjalikaushik@mdi.ac.in

Abstract

Cyberspace is a virtual environment where instantaneous communications are initiated and consumed using computer networks without any natural or artificial boundaries. These communications are not only an exchange of information but also a catharsis on the socio political environment of the real world. This explosion of electronic expression is often detrimental to the traditional secretive maneuvers of nation states and the exercise of its power. Unable to come to terms with the new reality nation states through legislative action or otherwise attempt to assert its sovereignty in the space that has no political and societal boundaries. This may lead to an encroachment on basic human rights that often have constitutional guarantees in the real world but may be violated in the online milieu. This paper attempts to investigate this issue in detail and evaluates whether nation states are using cyber-security as a propaganda tool to transgress on electronic expression.

Keywords

Cyber security, surveillance, privacy, civil liberties, censorship.

Introduction

More than 2.3 Billion people accounting for more than a third of the world’s population had access to Internet in 2011 and by 2017 these figures are going to grow to 70% of the world’s population (UNODC 2013). Interspersed within this revolution, cybercrimes are also rising exponentially. Several reports including one by Symantec suggests the gargantuan nature of the problem and the economic costs involved with it. This phenomenon is however not lost on national governments. They through legislative action or otherwise are intervening in this space and in doing so are often crossing the line. Existing literature suggests that there are myriad ways in which governments are intervening in the cyberspace. Surveillance is an instrument with which modern societies discipline and control populations; observation and inspection is used as a basis for judgment and intervention; enabling supposedly deviant individuals to be brought under corrective action to normalize them in accordance with dominant societal expectations (Foucault 1977). Indeed electronic evidence collected through surveillance is increasingly being used to construct offenders and mediate punishment (Pattavina 2004). ECHELON is a global network of electronic spy stations that can eavesdrop on communications through telephones, faxes and computers (Guardian 2001). It is also used to monitor organizations like Greenpeace and Amnesty International whose agenda may be critical to US political policies (Sykes 1999). In 2013 Reuters uncovered a secret unit of United States Drug Enforcement Agency known as the Special Operations Division (SOD) comprising of sleuths from Federal Bureau of Investigation, Central Intelligence Agency, National Security Agency etc. which provides information from wiretaps, Internet intercepts, and phone records to law enforcement agencies for criminal investigation of US citizens (Shiffman et al. 2013). China systematically deletes discussion on Tibet, Taiwan, Falun Gong Spiritual Movement and discussions on Democracy on the Internet (Martinsons 2005). In 2011 Scotland Police admitted to monitoring social networking sites in the wake of British Riots to anticipate spread of the urban unrest (Scotsman 2011). A direct consequence of this surveillance state is Self-Censorship imposed by Internet users upon themselves. This in fact is a bigger threat to Internet freedom than state censorship itself (Mihr 2013). Transparency Report published by Google indicates that most governments make content removal and use data requests and frequencies at which they make those requests are also similar on a per
capita basis (Wolf 2013). Invariably the reasons behind such surveillance are threat of terrorism and economic costs due to cybercrime. However, terrorist organizations cannot execute sophisticated cyber terror attacks due to limitations in gathering intelligence and penetrating systems, while the capability to launch major cyber-attacks are available to only a few countries (Siboni et al. 2013). In fact the spectre of Internet Terrorism is merely rhetorical embellishment and myth making (Yar 2006). In economic terms, various reports by computer security firms suggests the huge economic costs that are involved due to cybercrime but the computer security industry also has a vested interest in promoting this idea of imminent danger. And finally, even though human rights and fundamental freedoms are enshrined in the 1948 Universal Declaration of Human Rights and UN General Assembly resolution 68/167 has affirmed that “the rights held by people offline must also be protected online”, nation states are far from honoring such commitment. Personal data mining by US agencies for collecting, collating, cross matching data happens with near zero oversight of the US Congress and citizenry and without much accountability about how the data is put to use (McCullagh 2004). According to Civil Society Internet Society Advisory Council, the attempts by national governments including that of the OECD to link all cybersecurity issues to national security and warfare without specificity in contexts lead to bestowal of broad open ended powers to state agencies that threaten civil liberties in disproportionate ways. This is grossly detrimental to society as anonymity and privacy are extremely important to preserve diversity of speech (Wallace 1997) as they are rights and interests of individual and rights and interests of community as a whole (Wacks 1997).

Research Motivation

The Website of the UN Office of the High Commissioner for Human Rights states “In December 2013, the United Nations General Assembly adopted resolution 68/167, which expresses deep concern at the negative impact that surveillance and interception of communications may have on human rights”. It further says “The General Assembly called on all States to review their procedures, practices and legislation related to communications surveillance, interception and collection of personal data and emphasized the need for States to ensure the full and effective implementation of their obligations under international human rights law”. With this development this paper seeks to unravel the role of nation states in using cybersecurity as a propaganda tool by raising the spectre of threat to national security and economic wellbeing.

Methodology

The paper is based on exploratory research with data compilation from secondary sources. In order to collect data various research papers, books and journals have been referenced and data available in public domain has been accumulated.

Analysis and Findings

Research suggests that Cyber-Terrorism cannot cause widespread damage of life and property so as to hold it as justification for cyber surveillance. Cyber-Warfare on the other hand poses a far greater threat to national security than Cyber-Terrorism but ironically it is the preserve of nation states to wage such warfare. Non state actors have limited capacity in this space. Governmental narrative in this context seems rather illusory and indicates a systematic effort to establish a police state in the cyberspace. The below sections will try to statistically prove this.

Attack Trends

Threat to national security is mere myth making when it comes to Cyber-Attacks. Though data for Cyber-Warfare is not entirely reported, whatever is reported is a miniscule percentage if we take into account all forms of cybercrime reported in the public domain. A look at the data in Hackmageddon.com, a blog maintained by Paolo Passeri, reveals that both Cyber-Warfare and Cyber-Espionage account only for 10%
of all cyber-attacks reported in the media. In fact economic cybercrime accounts for around 60% of all cyber-attacks (Refer Figure 1).

Figure 1: Breakup of Cyber-Attacks by Type in 2013 and 2014 (Hackmageddon.com 2014)

Even military targets of Cyber-Attacks account for merely 2% of all forms of cyber-attacks. Academic institutions are subjected to more cyber-attacks than the armed forces. Significantly, most of the brunt of cyber-attacks is borne by businesses rather than governments. This reflects the economic nature of cyber-attacks rather than as an instrument of warfare or terrorism (Refer Figure 2).

Figure 2: Proportion of Cyber-Attacks Targets in 2013 and 2014 (Hackmageddon.com 2014)
The prevalence of economic cybercrime as the most widely used attack vector in guided more by the lure of economic benefits than to cause widespread loss of lives. Attacks to disrupt economic wellbeing can definitely be crippling for a nation state as seen in Estonia but economic coercion is still not considered as a use of force under Article 2(4) of the UN Charter.

**Economic Impact**

Considerable work has been done to estimate the cost of cybercrime. A few of the studies exaggerate the actual cost of cybercrime. The reason for such a narrative is to amplify the impact and secure the economic future of cybersecurity firms, who in most cases conduct such studies. There is definitely some doubt surrounding the veracity of such studies in the backdrop of an expanding cybersecurity market. IDC estimates that it is going to reach $42 Billion by 2017. But if we put the actual estimates by one of the firms, Symantec, into perspective and compare them with organized crime the economic costs of consumer cybercrime is much lower than that due to other forms of crime. In 2012 cybercrime cost was one fifth the cost of private sector corruption in developing economies. Economic cost of cybercrime in 2012 and 2013 according to estimates of Symantec is around 5% of the total loss due to organized crime estimated by UNODC in 2009 (Refer Figure 4).

![Figure 4: Comparison of Economic Cost of Cybercrime against other forms of crime (Symantec 2013; CSIS 2014; CNBC 2013 and UNODC 2011)](image)

Coincidentally, the geography wise estimates of Symantec of Consumer Cybercrime are closely comparable with just retail profit from cocaine trafficking in those geographies (Refer Figure 5).

![Figure 5: Comparison of geography wise Economic Cost of Cybercrime against Cocaine trafficking (Symantec 2013 and UNODC 2011)](image)
Data shows that cocaine abuse is more lethal than cybercrime and the economic costs of such abuse are also enormous. Even then in recent years tackling cybercrime is given more priority by governments than drug abuse. US Budget data suggest the asymmetry in priority accorded to tackle drug abuse compared to Intelligence gathering. The US Government spends almost twice the money in National Intelligence Program than it spends on Drug Control (Refer Figure 6).

![US Federal Spend Comparison on Drug Control and Surveillance (Billion USD)](image)

**Figure 6: US Federal Spend on National Intelligence and Drug control (Office of the Director of National Intelligence 2013 and Office of National Drug Control Policy 2014)**

How the money allocated for the security agencies is spent is not divulged and makes up the top secret “Black Budget” (Washington Post 2013). Again data estimates by another firm, McAfee, suggest that the cost of cybercrime as a percentage of GDP in countries across the world is a mere 1%. If we calculate the cost estimates of cybercrime as a percentage of the Internet Economy in most countries, it is below 15% of the total Internet Economy (Refer Figure 7).

![Cybercrime cost as a % of GDP and Internet Economy (2013)](image)

**Figure 7: Economic cost of Cybercrime as a percentage of GDP and Internet Economy (CSIS 2014 and BCG 2012)**

**Crime Incidence**

In most countries incidence of cybercrime is not recorded. But data that is available show that the incidence of cybercrime against other violent or property crimes is miniscule. In US it is around 3% of total crimes. In India it is less than 1% and in Germany it is around 4% (Refer Figure 8).
It would be interesting to see the ratio in EU when Eurostat publishes the data. But the argument that most of cybercrime remains unreported also holds true for other forms of crime as well. Again if we look into year on year data reported in Hackmaggedon.com and IC3 it is apparent that cybercrime is declining (Refer Figure 9).

This data is indicative and it would be interesting to see country wise year on year data to draw a conclusive inference. But it can be safely said that at least in the US complaints to IC3 has a declining trend. A look at the data reported by CERT in various countries also suggests that the crime rate of cybercrime when compared with rates of other forms of Crime is miniscule. In India CERT Incidents are the lowest compared with other crimes with crime against women is six times as much even when most of such violence perpetrated against women goes unreported. Japan, where crime per capita is amongst the lowest in the world, CERT incidents closely match crime against women and is higher than the homicide rate. The Japanese government should spend more resources on tackling theft which is almost eighty five times more than CERT incidents. Brazil has a CERT incident rate that is much higher than that of both homicide and crime against women but is dwarfed by theft and robbery rate. In US, crime against women is twice as much than CERT incidents but homicide again is a lesser reported crime. Like Japan and Brazil, theft is huge in US. All this data certainly suggests that there are other severe forms of menace to society than only cybercrime (Refer Figure 10).


**State Action**

Government action in cyberspace has some undesirable manifestations in surveillance and content control. Data from Transparency Reports suggest that most of such actions by governments are without any judicial oversight. On average below 10% of Removal Request received by Google are backed by Court Orders or Warrants. The Top 10 countries in requesting such removal are all democratic regimes (Refer Figure 11).

Ironically, National Security is not the basis for such removal requests. Rather the most important reason is Defamation. National Security as a cause of Removal Requests is on an average less than 4% of all such requests (Refer Figure 12).
Ironically the number of Removal Requests due to Government Criticism is similar to the number of requests due to National Security received by Google. And such Removal Requests due to government criticism are not restricted to non-democratic regimes. It is also a characteristic of democratically elected regimes. World's Largest Democracy, India was the second largest requester in 2011 (Refer Figure 13).

A similar scenario exists in User Data Requests as well. The Top 5 Countries in User Data Requests received by Google are all democratic countries. Barring United Kingdom all the other 4 countries have raised the frequency of their requests in the last 3 years (Refer Figure 14).
Data from the past few years actually shows a rising trend in Content Removal and User data requests. This is corroborated not only by Google but Microsoft as well. Again only a fraction of such requests are backed by Court Orders or Warrants (Refer Figure 15).

![Figure 15: Trends in Transparency Reports (Google 2013 and Microsoft 2013)](image)

These governmental transgressions are corroborated by government data itself. Though most governments do not reveal such data, the data that has been released till now at their own volition or due to lawsuits filed in the court of law portrays the staggering scale of surveillance conducted by government agencies (Refer Figure 16).

1. In US every 4 out of 1000 citizens are snooped.
2. In UK every 8 out of 1000 citizens are snooped.
3. In Australia every 30 out of 1000 citizens are snooped.
4. In India every 8 out of 100000 citizens are snooped (Refer Figure 17).

![Figure 16: Country wise Communication Interception per 1000 Inhabitants (ACMA 2013; Australian Bureau of Statistics 2013; UK Interception of Communications Commissioner 2013; UK Office of National Statistics 2013; ACLU 2012 and US Census Bureau 2013)](image)
The most alarming trend among all this is the use of Warrantless surveillance. In US Wiretapping is authorized by the court of law and do not show a significant uptrend in the last few years. But warrantless snooping like Pen Registers and Trap & Trace devices are increasing at a breakneck speed (Refer Figure 18).

**Figure 177: RTI Response by Ministry of Home Affairs, India (SFLC 2014)**

In this section, we review legislations across various countries that happen to infringe on online expression. It is without doubt that such legislations exist in most countries whether they are democratic or not.

**India**

The parent legislation that governs the Internet in India is the Information Technology Act, 2000 (“IT Act”). There are certain sections in the IT Act that abet electronic surveillance. Under Section 5(2) of the IT Act read with Rule 419-A (1) under sub-section (2) of Section 5 of the Indian Telegraph Act, 1885, either “the Secretary to the Government of India in the Ministry of Home Affairs in the case of Government of India and by the Secretary to the State Government in-charge of the Home Department in the case of a State Government” or a person above the rank of Joint Secretary, in “unavoidable circumstances” of emergent cases like remote areas or for operational reasons and authorized by the respective government,
during a public emergency or in the interest of public safety, is empowered to issue a written order
directing an communication interception, if the official believes that it is imperative to do so in the
“interest of sovereignty and integrity of India, the security of the State, friendly relations with foreign
states, public order”, or the prevention of incitement of offences. Section 69 of the IT Act allow authorized
government officers to intercept or monitor information transmitted, generated, received or stored in any
computer and requires service providers to extend all equipment and technical assistance to the
authorized government officer to intercept the information. All these provisions are further supported by
various rules.

**Information Technology (Procedure and Safeguards for Interception, Monitoring and
Decryption of Information) Rules, 2009:** These Rules lays down the procedure that the government
should follow while interception, monitoring or decryption of specific information stored, generated,
transmitted or received in any computer resource under order issued by a competent authority.

**Information Technology (Procedure and Safeguards for Monitoring and Collecting Traffic
Data or Information) Rules, 2009:** These Rules lays down the procedure that the government should
follow in monitoring and collection of traffic data or information by an agency of the government under
authorization by a competent authority for purposes related to cyber security.

**Information Technology (Procedure and Safeguards for Blocking for Access of
Information by Public) Rules, 2009:** These Rules lays down the procedure that the government
should follow for the purposes of issuing direction for blocking access by public any information
generated, transmitted, received, stored or hosted in any computer resource under order from a
Designated Officer appointed by the Central Government through notification in the Official Gazette.

**United States**

In US more than 50 statues address the concerns of Cybersecurity either directly or indirectly (Fischer
2013). A few notable legislations in the United States directly infringe on Internet freedom and to that
effect the National Security Agency is the primary agency tasked to gather Signals Intelligence (SIGINT).
It runs mass surveillance programs viz. PRISM, ECHELON among others. Broadly three laws govern
network surveillance in the United States.

**Communications Assistance for Law Enforcement Act of 1994 (CALEA):** This act directs
telecommunications carriers to assist law enforcement agencies to perform electronic surveillance and
requires the telecommunications industry to design and develop equipment that supports authorized
electronic surveillance over telephone, Internet and VOIP networks.

**USA PATRIOT Act of 2001:** This act authorizes various law enforcement agencies to undertake roving
wiretaps, search of business records and conduct surveillance of lone wolves. The act was hastily passed
after 9\11 terrorist attacks and allows the use of National Security Letters by the Federal Bureau of
Investigation to eavesdrop on personal information without court order.

**Foreign Intelligence Surveillance Act of 1978 (FISA):** This act provides a statutory framework for
federal agencies to conduct electronic surveillance by utilizing warrantless pen registers and trap & trace
devices to collect foreign intelligence on foreign powers and agents of foreign powers including American
citizens and permanent residents who are suspected of espionage or terrorism.

**China**

China is by far the most extreme case of Internet control. Since 1995 around 60 sets of regulations have
been passed to control the Internet as hallmark of a closed ideology propagated by the authoritarian
regime in place in China (Human Rights Watch 2009). Almost all Internet dissidents are charged under various sections of the Criminal Code and serve incarcerations ranging from two to four years and in some cases even death penalty. In 1994 the State Council passed the regulation “PRC Regulations for the Safety Protection of Computer Information Systems” that gave wide ranging powers to the Ministry of Public Security to supervise the cyberspace. The Article 5 of the “Computer Information Network and Internet Security, Protection and Management Regulations” issued by the Ministry of Public Security bans the dissemination and retrieval of any information on the Internet that incites the overthrow of the Socialist System. Article 8 of the same regulation requires service providers to accept supervision, inspection and guidance from the Public Security organization on digital content. The “Measures for Managing the Internet Information Services” and “Telecommunications Regulations Of The People’s Republic Of China” passed into law by the State Council in 2000 requires service providers to keep record of Internet or Telecommunication Network access by users and restrict transmission of material that jeopardizes national security, reveals state secrets, subverts state power, or undermines national unity. Similar is the case for “State Secrets Protection Regulations for Computer Information Systems on the Internet” issued by the Bureau for the Protection of State Secrets in 2000. Broadly three laws govern the Internet in China.

**Temporary Regulation for the Management of Computer Information Network International Connection:** Passed in 1996 by the 42nd Standing Convention of the State Council, it gives responsibility to the Ministry of Public Security to supervise the Internet and restricts users from establishing direct International connections by themselves. Consequently all Internet traffic is routed through State approved Internet Service Provides viz. ChinaNet, GBNet, CERNET, and CSTNET.

**Ordinance for Security Protection of Computer Information Systems:** This regulation deals with the enforcement of the above mentioned legislation by the Ministry of Public Security giving it powers to investigate and prosecute any violations to maintain national sovereignty.

**Computer Information Network and Internet Security, Protection, and Management Regulation:** Passed in 1997 this legislation specifically focuses on Internet Censorship. It says “No unit or individual may use the Internet to create, replicate, retrieve, or transmit the following kinds of information: Inciting to resist or breaking the Constitution or laws or the implementation of administrative regulations; Inciting to overthrow the government or the socialist system; Inciting division of the country, harming national unification” and “Injuring the reputation of state organizations; Other activities against the Constitution, laws or administrative regulations”. To enforce this censorship of the Internet the Ministry of public Security instituted the “Golden Shield Project” in 1998 better known as “The Great Firewall of China”.

**Australia**

**Telecommunications Act 1997:** Telecommunication Carriers and service providers have obligations under section 313(3) to provide necessary assistance to law enforcement agencies for interception of customer communications for the purposes of enforcing the criminal law and laws imposing pecuniary penalties, protecting public revenue or safeguarding national security.

**Telecommunications (Interception and Access) Act 1979:** Under Chapter 2, Part 2-2, the law enables law enforcement agencies to intercept live communications under warrant issued to the Australian Security Intelligence Organization.

**The Australian Security Intelligence Act 1979:** This act allows Australian Security Intelligence Organization to employ listening devices under warrant issued by the Minister upon application by the Director General on persons suspected of activities prejudicial to security.
Germany

The German Telecommunication Act (Telekommunikationsgesetz): Under Sec. 110 and Sec. 3 of the act, telecommunications operators are required to maintain technical and organizational capabilities to execute interception measures expressly provided for by law without any delay.

Federal Criminal Police Office Act: Under Sec. 20l interception orders are granted by court order on request by the President of Federal Criminal Police Office. The President of the Federal Criminal Police Office himself can also grant interception orders in case of imminent danger to the safety of Federal Republic of Germany and the life of a person or for the purpose of defending against terrorist aggression subject to judicial approval.

United Kingdom

Regulation of Investigatory Powers Act 2000 (RIPA): Under s.5 the Secretary of State is given the power to issue the interception of communication in interests of national security, prevention of crime or economic wellbeing of United Kingdom where the warrant is proportionate with the intended purpose.

Communications Act 2003: Under Section 132 the Secretary of State may require Office of Communications, independent regulator and competition authority for the UK communications industries, to issue a directive to suspend or restrict the network, services or facilities of an electronic communications network provider or service provider in interest of public safety, public health or national security.

If we now look at the laws of these countries through the prism of human rights it is evident that though all countries have ratified the International Covenant on Civil and Political Rights with the exception of China, their laws may be in conflict with Article 17 of the Treaty which states that “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” and “Everyone has the right to the protection of the law against such interference or attacks” (Refer Table 1).

<table>
<thead>
<tr>
<th>Policy Implications</th>
<th>India</th>
<th>US</th>
<th>China</th>
<th>Australia</th>
<th>Germany</th>
<th>UK</th>
</tr>
</thead>
<tbody>
<tr>
<td>Democratic Regime</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Ratification/Accession of International Covenant on Civil and Political Rights</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Communication Interception and Surveillance</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Warrantless Monitoring without Judicial Oversight</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Internet Censorship</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>National Security or Public Order as reason for Interference</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Mandatory Internet Service Provider cooperation</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Table 1: Policy Implications of Laws impacting Cyberspace in Different Countries

Conclusion

This paper has tried to unravel state action on cyberspace which often runs counter to the concept of civil liberties. It indicates that in terms of both national security and economic impact, cybercrime represent a very nominal threat vector. Also cybercrime as compared with other forms of crime is again nominal. Finally, cyber laws and policies of different countries need to be more nuanced such as to allow space for civil liberties. Overall, the propaganda surrounding the malaise of cybercrime seems to be more hype than
real. We already have examples of countries who have transgressed into electronic expression in cyber space. Therefore UN has a valid reason to raise a red flag on this unfolding issue.

References

11. UNODC. 2011. The Transatlantic Cocaine Market
State Transgression on Electronic Expression