Surveillance study

The surveillance and investigatory powers have the potential to impinge on a variety of human rights and intents including the right to private life home and communications and the right to protection of personal data. The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual Use Goods and Technologies points out the need for directives on the use of technology so that human rights infringements do not become the norm. The social effect of technological advances is that we now live in a world of ubiquitous computing. This has resulted in all aspects of our lives revolving around digital technologies. A paradox of digital technologies is how digital technologies make our lives easier on the other hand make our lives impossible due to the uncertainties brought about by the need for surveillance.

Globalization has brought about the emergence of global supply chains and the opening up of national markets proliferation of digital technologies. This has come at a cost, these are emerging treads of

* Governments globally have had to conduct mass surveillance programs outside existing domestic legal framework. Some governments have adopted laws that legalese post fecto these programs.
* Governments have placed their intelligence sharing practices over legal principles. This has led to failure of adequate safeguards and oversight leading to privacy interference.
* International human rights bodies and experts have pointed out how mass surveillance has violated human rights in most Countries. The UN Special Rapporteur on counter terrorism has noted how mass surveillance of digital content and communications data presents a serious challenge to the establishment on international law norms.

In 2016 the UN High Commissioner on Human Rights reiterated that “mass secret surveillance is not permissible under international human rights law an individual necessity and proportionality analysis would not be possible in such context”. The view that technological development, in particular communications and information technology may give raise to challenges. Surveillance in contrast to providing security by ensuring protection of the right to privacy in the context of protection and promotion of human rights.

It’s important to highlight the need for data protection legislation that takes into consideration the EU legal regime.[[1]](#footnote-1) The rise in privacy issues arising from the exponential growth in consumer and mobile “new technologies” such as Global Position Systems and Application programs, termed as intrusive. The Ben Faiza v France case is an example were the Court held that there had been violation of Article 8 right to respect for private life. The investigation was infect hamper by the court decision regarding the law enforcement actions as violation of minimum protection given to someone in a democratic society. The use of new technology in transnational crime trends signals a new challenges for scholars as they shape, global relations. The increase in transnational crime has affected the interests of States because criminal activity occurs in more than one State are commonly carried out for the personal gain and profit. . International instruments including bilateral and multilateral agreement that address transnational crime form the European Union framework for tacking cybercrime.[[2]](#footnote-2)

An argument for cybersecurity comes about as a result of terrorism and the need for a more reactive high-level security response from the State and private companies. This should involve a diplomatic approach that involves EU member states taking into consideration the security interests for member states in light of the terrorist attacks no Belgium, France, Germany and the United Kingdom, shows the significance for Cyber security.

The revelations of Edward Snowden point out the need for privacy and surveillance to become topics for collaborations from business and International Human Rights Organisations in partnership with academia and civil society stakeholders on bring about an cyber security approach that ensures human rights are upheld. An argument for the growing number of governments having expressed genuine interest in collaborative international analysis of personal data model such as the EU model General Data Protection Regulation (GDPR) is becoming the norm. It’s important to point out how Human Rights Council and the United Nations General Assembly (2016) conducted workshops to allow for the exchange of thoughts, positions and draft for legal instruments for the formulation of models for domestic surveillance soft law and hard law from multilateral, international treaty engagement. The argument for cyber security is underpinned by the need for new legal measures that take into consideration legal regimes at the international level for the improvement of protection of privacy in response to the growing incidence of surveillance.[[3]](#footnote-3)

#  The case The General Data Protection Regulation is made due to argument on how complex understanding of privacy is understood from various from European Union member state to state data sharing within the European Union jurisdiction. The Centrum for Rattvisa v. Sweden is a complex case understanding within the context EU Fundamental Human of Rights Article 8 the right to privacy is in contrast to surveillance for security purposes. European Union interpretants privacy as a fundamental human right and the GDPR Article 50 as a means of giving the people their human rights. An argument is therefore made on how the EU views privacy and data security more rigorously than the United States, Canada and Mexico.[[4]](#footnote-4)

The main focus of the study the right to personal data protection in the context of European Union GDPR efforts to protect against data breaches. The manner and scope in which judges decide when privacy interests are at risk of being violated compromises have to be made within an investigation of Cyber Crime from a domestic legislative framework. An argument is made on how cyber security approach adopts a Counter Terrorism approach and see cyber-attacks as an act of terror ensuring international humanitarian law regime albeit protection of human rights.[[5]](#footnote-5) Data protection envisioned as a human right in Single Digital Market (SDM). It is vital to the relationship between privacy and freedom of religion, freedom of expression, freedom of flow of information and non-discrimination not be hampered by State of Surveillance Programs or policies.

The United Nations advocates for a model of legal instruments on surveillance and privacy that can be joined into national legislatures embodying the highest principles of international human rights law on privacy and surveillance in Single Digital Market. However noting with great concern the Special Rapporteur points out how abuses to the right to privacy haves been infringed upon.[[6]](#footnote-6) The revelations from Edward Snowden are a case in point were the United Nations sharing with the European Union raising awareness of the link between international peace and security, human rights and development. The GDPR Article 50 ensures development of international cooperation for more secure cyber network.

The global challenges in response to the global crises caused by transnational cyber-attack and threats to peace and security have not made administration of surveillance technology easier. The United Kingdom Cyber Security Breaches (2018) have shown an awareness of 38 per cent of Business and 44 per cent of charities are aware of GDPR.[[7]](#footnote-7)

In the European Union member states have signed the Budapest Convection established by the Council of Europe in 2017[[8]](#footnote-8). An argument is made on how on how collaborative approach to nationwide Distribution of Denial Service DDoS attack on public and private infrastructure can assist.[[9]](#footnote-9)Antony Giddens distinguishes risk from hazard or dangers posed by new technology highlighting the need for cybersecurity.[[10]](#footnote-10) EU member States should ensure appropriate steps to ensure personal data including confidentiality integrity accessibility and authenticity required by regulations such as GDPR Article 60. It important to highlight the challenges that cybersecurity faces at national regional and international level.[[11]](#footnote-11)The Ben Faiza v France is an example of the challenges raised at the United Nations General Assembly (2017) include principles for the protection of privacy in the Big Data context. The facilitation of cyber security research on de-identification and situations of de-identification failure. In the context of the EU Member State are required to ensure Article 32 Security of personal data and Article 33 Notification of personal data breach to the Supervisory authority. An argument of how cyber security under the Budapest Agreement ensures domestic legislation is coherent with international norms. The forum on “Development in a Changing World” formed an expert group of intergovernmental experts and Groups of Governmental Experts (GGE) made the argument how cybercrime and responses from Member states and the international community must include the private sector, Internet Service Providers (ISP).

# Privacy by Design (PbD) is interpreted too narrowly The European Union legal regime as revelled by the study has been interpreted too narrowly which could negatively affect online business purchases. The terms of privacy and data protection are interchangeable. Data minimisation has been linked to strong focus on reductionist view of privacy. Privacy by design is a technical approach which takes into consideration the state of the art technology to cover human rights, freedom of expression and protection from discrimination issues.

# Hence the need for the technical systematic specification from which need to caveat by legislation when privacy is invaded technically.[[12]](#footnote-12) The need for privacy by design (PbD) as a remedy to invation of privacy and unwarranted surveillance has proven to be a initiative that could meet UN Guiding Priciples on Business and Human Rights. Privacy by design has highlighted the need for regulatory regimes that involve the private sector and state. This is evident for the need for Single Digital Market asymmetries between the public policy makers in the human rights dominance and technical commercial sector. The digital age has increased transnational technological growth in witness the need for pooling of legislative control of criminal activities and human rights violation.

Recommendation

* The need for legal justification for the use of hacking to target journalists and human rights defenders in countries such as Bahrain México and Morocco need attention in a bid to uphold human rights.
* The need for bulk hacking to be investigated which involves allowing mass hacking to be investigated and were inappropriately conducted disallowed or conducted in accordance with Human Rights Standards.
* The High Commissioner should recognize that interference with privacy and fundamental rights well security risks posed by government hacking recommend that States should refrain from surveillance techniques.
* The High Commissioner should note the serious implications to privacy that come about as a result of monitoring publicly available information on social networking sites. The fact that data is publicly available does not justify unregulated and unchecked collection analysis processing.
1. see Council of Europe (2018) points out the necessity to secure human rights dignity and protection of the human rights and fundamental freedoms of every individual and the diversification intensification and globalisation of data processing and personal data [↑](#footnote-ref-1)
2. see Budapest Convention on Cybercrime Article 23 General Principles relating to international co-operation in accordance with provisions of chapter relevant international instruments on international cooperation in criminal matters. [↑](#footnote-ref-2)
3. see Human Rights Commission (2018) In light of terrorist attacks in Belgium, France, Germany and United Kingdom highlighted the need for high profile security [↑](#footnote-ref-3)
4. Kosseff (2017) the European Commission has to determine adequate protection for personal data by evaluating of nation’s rule of law respect for human rights, data protection regulation and international commitment to personal data. [↑](#footnote-ref-4)
5. See Department for Digital Culture Media and Sport (2018) points out how there is no statistically significant difference between business and charities, also see Centrum For Rattvisa v Sweden the court decided in in favour of the State discretionary powers in protecting national security in light of the present day threats to global terrorism and organised crime [↑](#footnote-ref-5)
6. see Big Brother Watch and others vs the United Kingdom (No.58170/13) Bureau of Investigative Journalism and Alice Ross v The United Kingdom (no.62322/14) 10 Human Rights Organistions and Others v. The United Kingdom (no.24960/15) highlights revelations from Edward Snowden electronic surveillance programmes used by US and UK bulk interception. [↑](#footnote-ref-6)
7. see National Cyber Security Centre (2018) point out the threat caused by phishing a type of social engineering where attackers influence users to do disclose information or steal sensitive data in the UK. [↑](#footnote-ref-7)
8. The Budapest Convention an act to deter action directed against the confidentiality integrity and availability of computer systems aimed at formulating National cyber security policy, networks and computer data that builds synergies with EU members. [↑](#footnote-ref-8)
9. EUCPN (2018) EUCPN Toolbox Series No 12 Cybersecurity and Safety Policies and Practices Brussels [↑](#footnote-ref-9)
10. see Maria Weimer *The Origins of Risk as an Idea and the Future of Risk Regulation*, New technology unregulated has the potentially uncontrollable hazard of the dark side of risk undesired outcomes in the form of cyber-attack or DoDDS. [↑](#footnote-ref-10)
11. GGE Report (2018) The failure of the Group of Government Experts to reach a consensus on the final report on synergy between all actors at the international level when it comes to information and communication technologies involve personal data. [↑](#footnote-ref-11)
12. General Data Protection Regulation Article 25 (3) An approach for takes in consideration certification pursuant to Article 42 based on demonstrating compliance with requirements as set out in (1) and (2) [↑](#footnote-ref-12)