OBSERVARE
Universidade Autónoma de Lisboa

e-ISSN: 1647-7251
Vol. 13, Nº. 1 (May-October 2022)

JANUS.NET
e-journal of International Relations

BALANCING THE PRIVACY V. SURVEILLANCE ARGUMENT: A PERSPECTIVE FROM THE UNITED KINGDOM

VAIBHAV CHADHA
vchadha@jgu.edu.in
Assistant Professor of Law at Jindal Global Law School, O.P. Jindal Global University (India). He holds a master's degree in Law from Queen Mary University of London and bachelor's degree in commerce as well as law from University of Delhi. He has written international articles on anticipatory bail law in India, copyright law and freedom of speech and expression. Before moving to academia, Vaibhav worked at the Offices of Advocate General of State of Nagaland, India, and Additional Solicitor General of India. His areas of interest include free speech, media law, and criminal law.

Abstract

In the aftermath of revelations made by ex-NSA employee Edward Snowden about violation of privacy of individuals by states in the name of surveillance, right to privacy became one of the highly debated rights. There is no doubt that the state must secure privacy of its citizens, but it also has a responsibility towards safety of the citizens. There exist different views related to privacy and surveillance. One view is that the state has no right to look into the private affairs of an individual while the other view is that there is no harm in putting someone suspicious under the surveillance as it is the duty of the State to prevent any untoward act in the society. Considering the contrasting views about privacy and surveillance, this article explores the position existing in the United Kingdom and aims to answer several questions pertaining to the Privacy v. Surveillance debate.

Keywords

Privacy; Surveillance; Investigatory Powers Act; General Data Protection Regulation and Data Protection

How to cite this article

Chadha, Vaibhav (2022). Balancing the Privacy v. Surveillance argument: a perspective from the United Kingdom. In Janus.net, e-journal of international relations. Vol13, Nº. 1, May-October 2022. Consulted [online] on the date of the last visit, https://doi.org/10.26619/1647-7251.13.1.12

Article received on August 15, 2021 and accepted for publication on January 27, 2022

BALANCING THE PRIVACY V. SURVEILLANCE ARGUMENT: A PERSPECTIVE FROM THE UNITED KINGDOM

VAIBHAV CHADHA

1. Introduction

Right to privacy remains one of the paramount possessions of human beings. Since its coming into existence, the right to privacy has momentously progressed and has developed into an established right across majority of modern democracies.[1] Right to privacy is granted under Article 12 of Universal Declaration of Human Rights 1948, which states that there shall be neither "arbitrary interference" with anyone's "privacy, family, home or correspondence" nor an attack on an individual's "honour and reputation". Article 17 of the International Convention of Civil and Political Rights 1966 provides that no one's "privacy, family, home or correspondence" shall be subjected to "arbitrary or unlawful" intrusion. The legal basis of privacy as a right in Europe evolves from Article 8(1) of the European Convention of Human Rights (ECHR), which provides for right to respect for private and family life and Article 8(2), which provides that there shall be no interference in this right by public authority except in accordance with law.

Right to privacy in Europe has been further strengthened with the enforcement of General Data Protection Regulation (GDPR) in May 2018. GDPR is one of the most stringent privacy and security laws in the world. Despite being enacted by the European Union (EU), it casts a duty on all organizations situated anywhere in the world as far as they "target or collect" data of people in the EU region. GDPR also imposes heavy fines against those violating the privacy and security standards laid down by it.[2]

There is an intrinsic relationship between privacy and national security because there are restrictions as to how much people are willing to trade privacy in pursuit of national security.[3] Article 23 of GDPR provides that subject to the union or member state law, rights given in Articles 12 to 22 (rights of data subject) and Article 34 (communication of a personal data breach to the data subject) can be restricted by way of legislative

1 Eric Caprioli, Ygal Saadoun and Isabelle Cantero, 'The Right to Digital Privacy: A European Survey' (2006) 3 Rutgers Journal of Law & Urban Policy 211.
2 'What is GDPR, the EU's new data protection law?' *GDPR.EU* available at https://gdpr.eu/what-is-gdpr/ accessed on 12 May 2020
3 Fred H Cate, 'Government Data Mining: The Need for a Legal Framework' (2008) 43 Harvard Civil Rights-Civil Liberties Law Review 435, 484.

measure on the grounds of national security, defence, public security and prevention, investigation, detection or prosecution of crimes.

In the United Kingdom (UK), Data Protection Act 2018 (DPA, 2018) was enacted to implement GDPR. Before enactment of the DPA 2018, Data Protection Act 1998 regulated the domestic processing of personal data by intelligence agencies. A new structure has been created by DPA 2018, which provides a distinct mechanism to supervise the processing of personal data by intelligence agencies. This mechanism is based on the international standards that will be laid out in a revised Council of Europe "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data" (the "modernised Convention 108"; amended Protocol was adopted by the Council of Europe on 18 May 2018). It is pertinent to note that national security does not come in the purview of European Union law. As a result, neither GDPR nor Law Enforcement Directive (LED) covers in its ambit the processing of personal data for the purpose of national security. Consequently, the terms of GDPR and LED were not intended to be applicable to processing of personal data by the intelligence agencies.[4] LED concerns with the processing of personal data with the motive of "prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties" by the competent authorities.[5]

A specific mechanism for the intelligence agencies is provided by Part 4 of the DPA 2018 (intelligence services processing). It warrants that the processing of personal data by intelligence agencies is subjected to suitable and corresponding standards that acknowledge the serious task of the intelligence agencies in dealing with present-day and prospective threats to national security.[6] Also, section 110 of the DPA 2018 provides exemption to intelligence agencies from certain provisions of the Act where it is essential to safeguard national security.

2. Background

Privacy concerns all individuals in their most personal and private affairs. It is a fundamental human right that remains under continuous threat due to the modern technological advancements.[7]

Privacy should not be considered as an individual right in opposition to the larger societal good. Issues of privacy require equilibrium at both edges of the scale as privacy entails safeguarding against a range of various dangers or troubles, the worth of privacy varies

[4] Home Office, Government of United Kingdom, *Data Protection Act 2018, Factsheet – Intelligence Services Processing,* p. 1, available at < https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/711233/2018-05-23_Factsheet_4_-_intelligence_services_processing.pdf > accessed on 19 June 2020.

[5] Directive (EU) 2016/680 of the European Parliament and of the Council (27 April 2016), p. 1.

[6] Home Office, Government of United Kingdom, *Data Protection Act 2018, Factsheet – Intelligence Services Processing,* p. 2, available at < https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/711233/2018-05-23_Factsheet_4_-_intelligence_services_processing.pdf > accessed on 19 June 2020.

[7] Ilina Georgieva, 'The Right to Privacy under Fire Foreign Surveillance under the NSA and the GCHQ and Its Compatibility with Article 17 ICCPR and Article 8 ECHR' (2015) 31 Utrecht Journal of International and European Law 104.

based on the specific trouble or danger that is being safeguarded. All privacy issues are not alike, and some issues are more dangerous than others; thus, an abstract value cannot be assigned to privacy.[8] The conflict between surveillance and privacy is a consequence of our vast troubles adjusting with progress in technology.[9]

The importance of the right to privacy was highlighted when ex – National Security Agency (NSA) employee Edward Snowden made revelations that under a secret order of a court, records of millions of US citizens were being collected by NSA indiscriminately irrespective of the fact whether those individuals were involved in any illegal act or not.[10] This led to a huge outcry amongst the public and there were strong objections raised to such surveillance by the state. Public felt it was an intrusion into their personal lives by the state and became more aware and cautious in issues pertaining to their privacy.

In our society, surveillance technology is prevalent and that often results in a strong debate between the advocates and opponents of surveillance technology. Specifically, government surveillance has been brought more and more under scrutiny of the public with supporters asserting that it enhances security while opponents denouncing it for infringing privacy.[11] From the viewpoint of a society, it is important to preserve requisite balance between security concerns and privacy and intrinsic civil rights of citizens.[12]

3. Surveillance by State Agencies

Surveillance is not only for the governments. A substantial wealth is generated by private companies by gathering, utilizing, and selling personal data of individuals.[13] Surveillance, in simple terms means "watching over". It relates to "monitoring, tracking, observing, examining, regulating, controlling, gathering data and invading privacy." The term surveillance originates from the French word "veiller" and the Latin word "vigilare."[14]

Professor David Lyon defines surveillance as "the focused, systematic and routine attention to personal details for purposes of influence, management, protection or direction." As per Professor Lyon, surveillance is "focused" as it pays attention on individuals. The term "systematic" denotes that scrutiny of personal details is intentional and relies on some "protocols and techniques" and by term "routine," Professor Lyon means that it happens in all modern societies as a 'normal' part of day to day life

8 Daniel J. Solove, "I've Got Nothing to Hide" and Other Misunderstandings of Privacy' (2007) 44 San Diego Law Review 745, 763.
9 H. Akin Ünver, 'Politics of Digital Surveillance, National Security and Privacy' (Centre for Economics and Foreign Policy Studies, 2018) 7.
10 Glenn Greenwald, 'NSA collecting phone records of millions of Verizon customers daily' *The Guardian* (United Kingdom 6 June 2013).
11 Michelle Cayford & Wolter Pieters, '*The effectiveness of surveillance technology: What intelligence officials are saying'* (2018) The Information Society 34(2), 88 DOI: 10.1080/01972243.2017.1414721.
12 Stefan Schuster, Melle Berg , Xabier Larrucea, Ton Slewe and Peter Ide-Kostic, 'Mass Surveillance and technological policy options: Improving security of private communications' (2017) 50 Computer Standards & Interfaces 76, 77.
13 Neil M Richards, 'The Dangers of Surveillance' (2013) 126 Harvard Law Review 1934, 1938.
14 Kelly Gates, 'Surveillance' in Laurie Ouellette and Jonathan Gray (eds), *Keywords for Media Studies* (NYU Press 2017) 186.

dependent on administrative set-up and certain information technology.[15] Surveillance, as per him, is also invariably attached to a particular "purpose."[16]

Surveillance is not only for the communist and dictatorial states. In the aftermath of 9/11 attacks, 2005 London bombings and various other heinous crimes, huge investments have been made even by democratic states in surveillance technologies.[17] Presently, surveillance includes technologies, forms, operations, and established code of procedure for replicating and scrutinizing pictures, sounds, scripts, and transaction- generated and different kinds of data.[18] Electronic surveillance is an advantageous instrument in the hands of law enforcement agencies. It can enhance security of citizens, assist in criminal investigations, and supply strong evidence in a prosecution.[19]

3.1. Investigatory Powers Act 2016

On 29 November 2016, the Investigatory Powers Act 2016 (IPA) came into force. To regulate the usage and oversight of investigatory powers by law enforcement and the security and intelligence agencies, the act lays out a new framework.[20] IPA repeals part one of Regulation of Investigatory Powers Act 2000 (RIPA), which had 25 sections and it replaces the same with 272 sections on interception regulation. Foremost objective of the IPA is to revamp the system under which law enforcement and intelligence agencies of the UK can be permitted to carry out "interception, equipment interference or bulk communications data acquisition."[21]

As Secretary of State is responsible for "security and terrorism"[22], he/she issues the "bulk equipment interference warrant" based on an application made by the head of the intelligence service.[23] However, the Secretary of State personally takes the decision of issuing a bulk equipment interference warrant.[24]

These specific and detailed provisions try to fill in the gap and seek to prevent misuse by providing a need for warrant from the Secretary of State before authorising any bulk equipment interference. This indicates that issuing of such warrants is well regulated and cannot be used indiscriminately by officials below Secretary of State without his authorization for purpose other than the one specified. Section 176 to section 183 of the Investigatory Powers Act 2016 deals with "bulk equipment interference warrants". "Bulk

15 David Lyon, *Surveillance Studies: An Overview* (1st edn, Polity 2007) 14.
16 David Lyon, *Surveillance Studies: An Overview* (1st edn, Polity 2007) 15.
17 Neil M Richards, 'The Dangers of Surveillance' (2013) 126 Harvard Law Review 1934, 1938.
18 Kelly Gates, 'Surveillance' in Laurie Ouellette and Jonathan Gray (eds), *Keywords for Media Studies* (NYU Press, 2017) 187.
19 Edward Balkovich, Don Prosnitz, Anne Boustead and Steven C Isley, 'The Electronic Surveillance Challenge' In *Electronic Surveillance of Mobile Devices: Understanding the Mobile Ecosystem and Applicable Surveillance Law* (2015) RAND Corporation 1.
20 Investigatory Powers Act, *available at* https://www.gchq.gov.uk/information/investigatory-powers-act accessed on 15 June 2020.
21 Thomson Reuters Practical Law, *Investigatory Powers Act 2016: Overview* by Practical Law Business Crime and Investigations, p. 1.
22 Secretary of State for the Home Department, Responsibilities https://www.gov.uk/government/ministers/secretary-of-state-for-the-home-department accessed 3 March 2020.
23 Investigatory Powers Act 2016, s 178.
24 Investigatory Powers Act 2016, s 182.

equipment interference warrant" authorises the person to whom it is addressed to obtain interference with any kind of equipment for the aim of obtaining "communications, equipment data and any other information."[25]

27 June 2018 onwards, under the IPA, the interception of communications operations became legitimized. Only Secretary of State can issue warrants authorising interception, and they are required to be ratified by an independent Judicial Commissioner from the Investigatory Powers Commissioner's Office. Prior to issuing of an interception warrant, the Secretary of State must "believe" that a warrant is "necessary" on some grounds and the interception corresponds to the purpose it aims to accomplish. Interception is considered "necessary" on the grounds of "national security", "economic well-being of the UK" or "prevention or detection of serious crime". To restrict the usage of intercepted information and associated communications data, IPA requires arrangement of safeguards.[26]

The IPA 2016 caused a noteworthy change in the way some investigatory powers are approved and supervised. The introduction of what it is informally called "double lock" method is the most remarkable change brought in by the IPA 2016. "Double lock" mechanism implies that following authorization by the Secretary of State, an IPA warrant cannot be issued unless a Judicial Commissioner authorises it.[27] The inception of 'double lock' mechanism has initiated a pivotal new feature to judicial oversight of the UK's intelligence and security agencies, giving the task of independently analysing approvals requested under the IPA 2016 to Judicial Commissioners.[28]

Hailing the passage of IPA 2016, Home Secretary Amber Rudd stated, "This Government is clear that, at a time of heightened security threat, it is essential our law enforcement, security and intelligence services have the powers they need to keep people safe." She further observed, "The internet presents new opportunities for terrorists and we must ensure we have the capabilities to confront this challenge. But it is also right that these powers are subject to strict safeguards and rigorous oversight." Pointing towards transparency and privacy protection set out in the Act, she asserted that "The Investigatory Powers Act is world – leading legislation that provides unprecedented transparency and substantial privacy protection."[29]

3.2. Operations by the State Agencies

Interception is a method where a person other than the sender or recipient of that communication oversees the communication during the course of its transmission with

[25] Investigatory Powers Act 2016, s 176.
[26] Investigatory Powers Act, *available at* https://www.gchq.gov.uk/information/investigatory-powers-act accessed on 15 June 2020.
[27] Government of UK, 'Annual Report of the Investigatory Powers Commissioner' (2018) p. 10, *available at* https://ipco.org.uk/docs/IPCO%20Annual%20Report%202018%20final.pdf accessed on 16 June 2020.
[28] Government of UK, 'Annual Report of the Investigatory Powers Commissioner' (2018) p. 9 [2.3], *available at* https://ipco.org.uk/docs/IPCO%20Annual%20Report%202018%20final.pdf accessed on 26 June 2020.
[29] Home Office (Government of UK), 'Investigatory Powers Bill receives Royal Assent' (28 November 2018) *available at* https://www.gov.uk/government/news/investigatory-powers-bill-receives-royal-assent accessed on 15 June 2020.

the purpose of making its contents accessible.[30] Employment of data mining technologies in national security is an effort to automate some systematic work to permit finer and well timed examination of prevailing datasets with the object of being able to avert terrorist activities by recognizing and categorizing several "threads and pieces of information," which may be in existence already but are overlooked due to use of methods of investigation that are traditional.[31]

A radical transformation in surveillance by state is ignited by the digital age, both in terms of how surveillance is carried out and the kinds of insights it is intended to promote. The transformation in surveillance by state is represented by the usage of "bulk communications data techniques" that comprise of extensive gathering, holding and successive analysis of communications data. Now, such techniques are an integral aspect of surveillance by state.[32] Contrary to the targeted data collection, bulk communications data surveillance denotes extensive "collection" and "retention" of communications data. It is used by both intelligence and law enforcement agencies today.[33]

Data mining is the method of exploring new information in the already existing data.[34] Data mining usually determines "patterns or relationships" in the data items or records, which were earlier not recognized but are disclosed in the data only.[35] Data mining provides favourable opportunities for overcoming the gap in the informational requirements of the government and the huge datasets of information available to it. The available data can be converted into knowledge with data mining.[36] The procedure of data mining essentially demands automatic review and assessment of profiles comprising personal information of various persons.[37]

A serious threat from surveillance is programmes like 'Data Mining.' 'Data mining' presents instruments for automatically analysing the data.[38] Huge quantities of data is retained by the government agencies, which then examines them with the intention of gaining knowledge for creation and storing of important information.[39] Interesting thing about data mining is that it aims to predict our future actions and those individuals who match some specific profiles are considered involved in "similar pattern of behaviour". In

30 Intelligence and Security Committee of Parliament: Privacy and Security: A modern and transparent legal framework (2015) 17 https://info.publicintelligence.net/UK-ISC-MassSurveillance.pdf accessed 12 June 2020.
31 KA Taipale, 'Data Mining and Domestic Security: Connecting the Dots to Make Sense of Data', (2003-2004) 5 Columbia Science and Technology Law Review 1, 21.
32 Murray D and Fussey P, "Bulk Surveillance in the Digital Age: Rethinking the Human Rights Law Approach to Bulk Monitoring of Communications Data" (2019) 52 Israel Law Review 31.
33 Daragh Murray and Pete Fussey, "Bulk Surveillance in the Digital Age: Rethinking the Human Rights Law Approach to Bulk Monitoring of Communications Data" (2019) 52 Israel Law Review 31, 36.
34 KA Taipale, 'Data Mining and Domestic Security: Connecting the Dots to Make Sense of Data', (2003-2004) 5 Columbia Science and Technology Law Review 1, 22.
35 KA Taipale, 'Data Mining and Domestic Security: Connecting the Dots to Make Sense of Data', (2003-2004) 5 Columbia Science and Technology Law Review 1, 22-23.
36 Tal Z Zarsky, 'Governmental Data Mining and its Alternatives' (2011) 116 Pennsylvania State Law Review 285, 294.
37 Tal Z Zarsky, 'Governmental Data Mining and its Alternatives' (2011) 116 Pennsylvania State Law Review 285, 295.
38 Stijn Vanderlooy, Joop Verbeek and Jaap van den Herik, 'Towards Privacy-Preserving Data Mining in Law Enforcement' (2007) 2(4) JICLT 202.
39 Stijn Vanderlooy, Joop Verbeek and Jaap van den Herik, 'Towards Privacy-Preserving Data Mining in Law Enforcement' (2007) 2(4) JICLT 202.

those circumstances, the actions that have yet not been committed would be difficult to refute and it shall be more onerous for us to dismiss future activity predictions done by data mining.[40]

Many privacy advocates warn that gathering and retaining of unlimited 'metadata' of communication activities of people by the government is the most intrusive form of surveillance.[41] Metadata, in simple terms, is data about data. Ordinarily, information comprises of semantic tags applicable to data. Metadata contains semantically tagged data, which are utilized to explain data.[42] Metadata is also known as 'communications data' and the UK High Court in *Davis and Others v Secretary of State for the Home Department* explained 'communications data' in the following words:

> *The phrase "communications data" does not include the content of a communication. Such data can be used to demonstrate who was communicating; when; from where; and with whom. They can include the time and duration of a communication, the number or email address of the originator and recipient, and sometimes the location of the device from which the communication was made. They do not include the content of any communication: for example the text of an email or a conversation on a telephone.*[43]

The court further stated that in the course of investigations concerning national security and organised and serious crime, the intelligence and law enforcement organizations use communications data. The data helps investigation agencies in identifying associates of a criminal nexus, placing them at particular locations at predetermined times and in some cases to comprehend criminal activity they are involved in.[44] When "combined" and "aggregated" to yield detailed record of communication and internet – based activity of an individual, communication data is considered specifically advantageous for the intelligence and security agencies.[45]

4. Evaluating the Privacy vs Security argument

A chilling effect is said to be created by surveillance when individuals desist from taking part in activities due to apprehension that some consequences will follow if they observe such activity.[46] Surveillance prevents an individual from enjoying his/her freedom to

[40] Daniel J. Solove, "I've Got Nothing to Hide" and Other Misunderstandings of Privacy' (2007) 44 San Diego Law Review 745, 764.
[41] Glenn Greenwald, 'NSA collecting phone records of millions of Verizon customers daily' (*The Guardian,* 6 June 2013) https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order accessed 4 March 2018.
[42] Tony Hey and Anne Trefethen, 'The Data Deluge: An e-Science Perspective', available at https://eprints.soton.ac.uk/257648/1/The_Data_Deluge.pdf accessed on 25 April 2020.
[43] Davis and Others v Secretary of State for the Home Department [2015] EWHC 2092 [13].
[44] Davis and Others v Secretary of State for the Home Department [2015] EWHC 2092 [14].
[45] Daragh Murray and Pete Fussey, "Bulk Surveillance in the Digital Age: Rethinking the Human Rights Law Approach to Bulk Monitoring of Communications Data" (2019) 52 Israel Law Review 31, 34.
[46] Daragh Murray and Pete Fussey, "Bulk Surveillance in the Digital Age: Rethinking the Human Rights Law Approach to Bulk Monitoring of Communications Data" (2019) 52 Israel Law Review 31, 43.

liberty and speech. One cannot move or speak freely when he/she knows that state is following him/her at each step and is seeing all his/her acts. This leads to creation of a society which is quite similar to the one described by George Orwell in the famous novel 'Nineteen Eighty-Four'. The society described by Orwell had a situation where everyone lived in the constant fear of being watched by the State at every moment and had to act or think in a way expected by the state and not in the manner; they themselves would like to think.[47] This Orwellian society restricts the movements, thoughts, conduct of citizens in their daily lives and makes them robots who are supposed to follow the instruction of the state, which can be very harmful for the existence of a free society itself.

In 2013, Edward Snowden exposed Government Communication Headquarters' (GCHQ) operation codenamed 'Tempora' that he termed as "the largest programme of suspicion less surveillance in human history".[48] Under the operation 'Tempora', large volumes of data taken from fibre optic cables could be stored for 30 days for analysing the data by the GCHQ. The data included phone records, email message contents, Facebook entries, internet history and many more details not only of the suspected targets but also of innocent people.[49] Finally, on 6 February 2015, the Investigatory Powers Tribunal held that the regulations that gave access to GCHQ to email and phone records intercepted by NSA breached Article 8 and Article 10 of the ECHR.[50]

The judiciary came forward and protected the rights of the citizens who were under threat from the state in matters relating to their privacy. The state may try to justify such massive and indiscriminate surveillance in the name of security and safety of citizens but it must not be forgotten that there must be drawn a line to prevent the state from interfering in personal activities of innocent citizens in the name of safety and security. Programmes like 'Tempora' give powers to the state agencies to collect mass data and provides them access to personal details like the email message.

We must never forget that government agencies do not comprise of one individual but many. There may be many officers working with integrity and would be following guidelines or safeguards provided under the statute while using the personal data for the purpose of surveillance. However, there remains a probability that some officers who may get access to such a high volume of data meant for security purpose may do away with safeguards provided during the period of "emergency or crisis" and misuse such data.[51] Misuse of data secured is not only an intrusion but an act which is illegal. The

47 Neil M. Richards, 'The Dangers of Surveillance' (2013) 126 Harvard Law Review 1934, 1948.
48 Ewen MacAskill, Julian Borger, Nick Hopkins, Nick Davies and James Ball, 'GCHQ taps fibre-optic cables for secret access to world's communications' (*The Guardian*, 21 June 2013) https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa accessed 13 May 2020.
49 Ewen MacAskill, Julian Borger, Nick Hopkins, Nick Davies and James Ball, 'GCHQ taps fibre-optic cables for secret access to world's communications' (*The Guardian*, 21 June 2013) https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa accessed 13 May 2020.
50 Owen Bowcott, 'UK-US surveillance regime was unlawful 'for seven years' *The Guardian* (6 Feb 2015) https://www.theguardian.com/uk-news/2015/feb/06/gchq-mass-internet-surveillance-unlawful-court-nsa accessed 13 June 2020.
51 Adam D. Moore, 'Privacy, Security and Government Surveillance: Wikileaks and the new Accountability' (2011) 25(2) Public Affairs Quarterly 141, 145.

most unfortunate part of data mining is that the individual or the masses who are under surveillance are not even aware that they are under surveillance and that their acts including google search, bank details and other details are being observed by the State. If such acts are to happen in vibrant democracies like the UK, then it would be difficult to imagine the worst forms of surveillance that might be carried out by the dictatorial regimes where such bulk interception may be misused to muzzle the voices opposing the government.

Article 8 of the ECHR is fundamental because it outlines one's right to have his/her privacy respected by any organization while at the same time it furnishes conditions under which the State is permitted and sometimes authorized to "exert certain prerogatives." "National security, public safety, [and] the prevention of disorder or crime" are among the grounds on which a state can intervene in the right to privacy. Thus, it can be suggested that for those who drafted the ECHR, security superseded privacy.[52]

The intelligence and security agencies are committed to a mission, ensuring safety and security of the citizens is the main reason for their role and assertion on the country's significant and governmental resources.[53] This suggests that the intelligence agencies need access to private information of an individual for securing the society and one must not worry if he is not committing any illegal act.

There is another argument that favours surveillance and holds view that there can be no intrusion of privacy by mere automatic gathering and organising of data. As the data gathered is in bulk, such data initially passes through the computers that search for phone number, names and other details of persons who are of intelligence worth to the government agencies. The automatic 'sifting' of data by the computer prevents perusal of private data by an intelligence officer and thus it does not intrude into privacy.[54] This argument speaks in favour of surveillance and assures that certain protocols are followed for surveillance so as not to intrude the privacy.

Many concerns have also been raised regarding the bulk interception capability of GCHQ and it has been alleged that it observes all communications on the internet. But as per the Intelligence and Security Committee of Parliament, that is not correct because GCHQ's bulk interception capability is used for only scrutinizing those individuals who pose threat or used for the object of creating new intelligence leads like tracking any cyber-attack or terror plot.[55] Another issue that report dealt with was a charge made against GCHQ that it does interception "indiscriminately". Refuting such allegation, the committee responded: *GCHQ first choose the bearers to access (a small proportion of those they can theoretically access) and then use specific selectors, related to individual*

[52] Eric Caprioli, Ygal Saadoun and Isabelle Cantero, 'The Right to Digital Privacy: A European Survey' (2006) 3 Rutgers Journal of Law & Urban Policy 211, 213.

[53] Charles D. Raab, 'Security, Privacy and Oversight' in Andrew W. Neal (ed) *Security in a Small Nation: Scotland, Democracy, Politics* (Open Book Publishers, 2017) 81.

[54] Richard A. Posner, 'Our Domestic Intelligence Crisis' *Washington Post* (21 December 2005) *available at* https://www.washingtonpost.com/archive/opinions/2005/12/21/our-domestic-intelligence-crisis/a2b4234d-ba78-4ba1-a350-90e7fbb4e5bb/accessed on 14 May 2020.

[55] Intelligence and Security Committee of Parliament: Privacy and Security: A modern and transparent legal framework (2015) 28, para F https://info.publicintelligence.net/UK-ISC-MassSurveillance.pdf accessed 15 May 2020.

targets, in order to collect communications from those bearers.[56] It clarified that it targeted the individuals and did not do surveillance at a massive scale that may have included several innocent persons and thus, maintained limits by not intruding their privacy.

The advantages of "bulk interception" can be seen from the report submitted by Intelligence and Security Committee of Parliament in 2015, which stated "We were surprised to discover that the primary value to GCHQ of bulk interception was not in reading the actual content of communication, but in the information associated with those communications."[57] Communications data surveillance virtually enables in keeping an eye on each and every action of all individuals, to uncover and assess their relationships with other individuals, and to attain extensive understanding into the lives of those individuals.[58]

These observations by the committee of Parliament try to instil a sense of security in minds of the citizens that they are not subject to absolute and unchecked bulk interception by intelligence agencies and these interceptions are motivated towards those suspects who pose threat to the UK.

It is important to mention that issue necessarily doesn't have to be of 'privacy' or 'security', as successful planning, consistent implementation, and meticulous supervision of extensive safeguard measures by law makers can harness the advantage of technology to achieve both privacy and security.[59]

5. Conclusion

It would not be correct to say that both privacy and surveillance are against each other, or one trumps the other, no state can deny the need of either absolutely. Unless the state has sufficient evidence of one being involved in a crime, the law enforcement agencies should refrain from intercepting communications of those individuals. 'Those who have nothing to hide have nothing to fear' argument does not give an absolute right to intelligence agencies to intercept all communications of citizens indiscriminately but only with checks and balances.

At the same time, we must not forget that terror plotting these days is not limited to physical locations but has expanded to the digital platforms as well, necessitating surveillance. Thus, the government, before framing more efficient and non-intrusive surveillance laws, must do due deliberations and consultations not only with law enforcement agencies but also with organisations outside the government.

---

[56] Intelligence and Security Committee of Parliament: Privacy and Security: A modern and transparent legal framework (2015) 28, para G https://info.publicintelligence.net/UK-ISC-MassSurveillance.pdf accessed 15 May 2020.

[57] Intelligence and Security Committee of Parliament, 'Privacy and Security: A modern and transparent legal framework' (2015) p. 32 [80].

[58] Murray D and Fussey P, "Bulk Surveillance in the Digital Age: Rethinking the Human Rights Law Approach to Bulk Monitoring of Communications Data" (2019) 52 Israel Law Review 31, 52.

[59] John P. Heekin, 'Leashing the Internet Watchdog: Legislative Restraints on Electronic Surveillance in the U.S. and U.K.' (2010) 28(1) American Intelligence Journal 40.

References

Balkovich, Edward; Prosnitz, Don; Boustead, Anne and Isley, Steven C. (2015). 'The Electronic Surveillance Challenge' In *Electronic Surveillance of Mobile Devices: Understanding the Mobile Ecosystem and Applicable Surveillance Law*. RAND Corporation 1.

Balkovich, Edward; Prosnitz, Don; Boustead, Anne; Isle, Steven C. (2015). Electronic Surveillance of Mobile Devices: Understanding the Mobile Ecosystem and Applicable Surveillance Law. RAND Corporation 1, https://www.rand.org/content/dam/rand/pubs/research_reports/RR800/RR800/RAND_RR800.pdf

Berger, J.M. and Morgan, Jonathon (2015). 'The ISIS Twitter Census Defining and describing the population of ISIS supporters on Twitter'. The Brookings Project on U.S. Relations with Islamic World (Analysis Paper) 2.

Bowcott, Owen (2015). 'UK-US surveillance regime was unlawful 'for seven years' In *The Guardian* (6 Feb 2015).

Caprioli, Eric; Saadoun, Ygal and Cantero, Isabelle (2006). 'The Right to Digital Privacy: A European Survey'. In *Rutgers Journal of Law & Urban Policy*, Vol 3:2, 211-218.

Cate, Fred H. (2008). 'Government Data Mining: The Need for a Legal Framework' (June 2008). In Harvard Civil Rights-Civil Liberties Law Review (CR-CL), Vol. 43, No. 2, 2008, Available at SSRN: https://ssrn.com/abstract=1151435

Cayford, Michelle & Pieters, Wolter (2018). '*The effectiveness of surveillance technology: What intelligence officials are saying'.* In The Information Society 34(2), 88 https://doi.org/10.1080/01972243.2017.1414721.

Davis and Others v Secretary of State for the Home Department (2015). EWHC 2092. https://vlex.co.uk/vid/david-davis-mp-and-793030889

Dearden, Lizzie (2017). 'Khalid Masood: Suspected Isis supporter used WhatsApp two minutes before London attack'. In *The Independent* (24 March 2017).

Directive (EU) 2016/680 of the European Parliament and of the Council (27 April 2016), p. 1., http://data.europa.eu/eli/dir/2016/680/oj

Feldstein, Steven (2019). *The Global Expansion of AI Surveillance*. Washington DC: Carnegie Endowment for International Peace. Working paper 11.

Gates, Kelly (2017). 'Surveillance'. In Laurie Ouellette and Jonathan Gray (eds), *Keywords for Media Studies*. NYU Press: 186.

Greenwald, Glenn (2013). 'NSA collecting phone records of millions of Verizon customers daily'. In *The Guardian* (6 June 2013).

Hey, Tony and Trefethen, Anne (2020). 'The Data Deluge: An e-Science Perspective', available at https://eprints.soton.ac.uk/257648/1/The_Data_Deluge.pdf, accessed on 25 April 2020.

Home Office, Department for Digital, Culture Media & Sport. (2018). *Data Protection Act 2018, Factsheet – Intelligence Services Processing.* Government of United Kingdom. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/711233/2018-05-23_Factsheet_4_-_intelligence_services_processing.pdf.

Ilina Georgieva, 'The Right to Privacy under Fire – Foreign Surveillance under the NSA and the GCHQ and Its Compatibility with Art. 17 ICCPR and Art. 8 ECHR' (2015) 31(80) Utrecht Journal of International and European Law 104, DOI: http://dx.doi.org/10.5334/ujiel.cr

Intelligence and Security Committee of Parliament. (2015). *Privacy and Security: A modern and transparent legal framework.* Government of United Kingdom. https://isc.independent.gov.uk/wp-content/uploads/2021/01/20150312_ISC_PSRptweb.pdf.

Investigatory Powers Commissioner's Office. (2018). *Annual Report of the Investigatory Powers Commissioner's Office*. Government of the United Kingdom. https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/IPCO-Annual-Report-2018-final.pdf.

Moore, Adam D. (2011). 'Privacy, Security and Government Surveillance: Wikileaks and the new Accountability'. Public Affairs Quarterly, Vol 25, N2: 141-156.

Posner, Richard A. (2005). 'Our Domestic Intelligence Crisis'. In *The Washington Post* (21 December 2005).

Raab, Charles D. (2017). 'Security, Privacy and Oversight' in Andrew W. Neal (ed) *Security in a Small Nation: Scotland, Democracy, Politics* (Open Book Publishers 2017), https://www.openbookpublishers.com/resources/9781783742684/Security-Small-Nation-ch3.pdf.

Investigatory Powers Act

GDPR.EU (2022). 'What is GDPR, the EU's new data protection law?', https://gdpr.eu/what-is-gdpr/

Heekin, J. P. (2010). Leashing the Internet Watchdog: Legislative Restraints on Electronic Surveillance in the U.S. and U.K. *American Intelligence Journal*, *28*(1), 40–58. http://www.jstor.org/stable/44327129.

Lyon, D. (2007). *Surveillance Studies: An Overview*. Polity. University of Michigan: Wiley, 1st ed.

MacAskill, Ewen; Borger, Julian; Hopkins, Nick; Davies, Nick and Ball, James (2013). 'GCHQ taps fibre-optic cables for secret access to world's communications'. In *The Guardian* (21 June 2013).

Murray, D., & Fussey, P. (2019). Bulk Surveillance in the Digital Age: Rethinking the Human Rights Law Approach to Bulk Monitoring of Communications Data. *Israel Law Review, 52*(1), 31-60. https://doi.org/10.1017/S0021223718000304.

Palmer, Danny (2019). 'What is GDPR? Everything you need to know about the new general data protection regulations' (*ZDNet*, 17 May 2019), https://www.zdnet.com/article/gdpr-an-executive-guide-to-what-you-need-to-know/

R (Liberty) v. Secretary of State for the Home Department and another (National Union of Journalists intervening), EWHC 2057 (Admin). (2019).

Richards, Neil M. (2013). 'The Dangers of Surveillance'. In Harvard Law Review, Vol 126, N7: 1934.

Schuster, Stefan; Berg, Melle; Larrucea, Xabier; Slewe, Ton and Ide-Kostic, Peter (2017). 'Mass Surveillance and technological policy options: Improving security of private communications'. Computer, Standards & Interfaces, Vol. 50: 76-82, https://www.sciencedirect.com/science/article/pii/S0920548916300988.

Solove, Daniel J. (2007). 'I've Got Nothing to Hide" and Other Misunderstandings of Privacy'. In San Diego Law Review, 44: 745.

Szeghalmi, Veronika (2015). 'The Definition of the Right to Privacy in the United States of America and Europe'. In Hungarian Yearbook of International Law and European Law, 397.

Taipale KA (2003) Data mining and domestic security: connecting the dots to make sense of data. Columbia Sci Technol Law Rev 5(2):83.

Thomson Reuters Practical Law, *Investigatory Powers Act 2016: Overview* by Practical Law Business Crime and Investigations, p. 1.

Ünver, H. Akin (2018). 'Politics of Digital Surveillance, National Security and Privacy'. Centre for Economics and Foreign Policy Studies, 2018/2: 17.

Vanderlooy, S., Verbeek, J. P. G. M., & van den Herik, H. J. (2007). Towards privacy-preserving data mining in law enforcement. *Journal of International Commercial Law and Technology*, *2*(4), 202-210.

Zarsky, Tal Z. (2011). 'Governmental Data Mining and its Alternatives', Pennsylvania State Law Review, Vol116:2, 285-330.