To what extent has the Investigatory Powers Act 2016 achieved an appropriate balance between the competing interests of Privacy and Intrusion?

By

Tommy Chadwick

Canterbury Christ Church University

Thesis submitted for the degree

of

MSc by Research

2017

Abstract

Investigating how recent Privacy and Intrusion laws have changed to affect individual's rights around the areas of terrorism, data retention and the recent Investigatory Powers Act. Accompanying this, research into how participants perceive storing personal sensitive data and whether this should be held by a specific authority is considered. This assessment on whether the public should have their information stored and investigated, with the aim to aid in the prevention/detection of serious crime and terrorism is needed. The necessity to find a balance between both privacy and intrusion is key in a society with expanding modern technologies. By analysing past legislation to show where the Government has misused its powers to find specific crimes will give an understanding on the next step to combatting threats against the nation, while also weighing in on how to combat the growing intrusion against ones privacy rights. The balance needed must ensure privacy, and the correct processes to ensure national security is upheld.

Acknowledgements

To my supervisors, Tom* and Kos*for all your help and support. To my father, Keith and step-mother, Mandy for encouraging me to continue in life regardless of the circumstances. To my friends; Jacob, Karl, the Sophie's, and Skye for ensuring whenever I lost my path to get straight back onto it. I would also like to thank Canterbury Christ Church University for giving me the facilities to achieve my degree.

---

* Tom Mortimer (Director of Law, Criminal Justice & Computing, Canterbury Christ Church University, UK)
* Dr Konstantinos Siliafis (Senior Lecturer in Law, Canterbury Christ Church University, UK)

Chapter Contents

1 – Introduction

The investigatory Powers Act 2016 is the newest piece of legislation regarding privacy and intrusion rights. The United Kingdom created this to counter the rise of terrorism threats over the last two decades. As terrorism has continued to grow the Government has implemented newer types of legislation to try to combat the threat and the modifications of the problems occurred through modern technology. This has been done to ensure society is protected from the threats. The problem is that the Government is trying to safeguard the public, by using their information to intercept criminal or terrorist activity and prevent any action. This is where the intrusion element comes into force, as individual's information is being taken to try to counter the ongoing threats, while privacy rights are essential to ensure the protection of personal sensitive data.

The proposals the Government implemented were to "investigate, prevent and supress terrorism"[3], and has since been included to serious crime[4]. One of the first anti-terror laws[5], had implications for privacy and intrusion based on the regulation of communications data.[6] This is due to powers within the Act that allow the Government to investigate any data they have on an individual, use it to counter crime/terrorism and keep the information until it is no longer needed. Privacy international has deemed this as an intrusive act against society, especially when those investigated may not have committed any crimes[7].

[3] European Council, 'Declaration on Combating Terrorism' [2014]
[4] One example, in response to September 11th was when the UK Parliament introduced the Anti-Terrorism, Crime, and Security Act 2001 only two months after the attacks.
[5] Regulation of the Investigatory Powers Act 2000
[6] Anti-Terrorism, Crime, and Security Act 2001 Pt 11
[7] Privacy International, 'Mass Surveillance' https://www.privacyinternational.org/node/52 accessed 27/06/2017

The Anti-Terrorism, Crime, and Security Act is one example where legislation has been reformed due to its incompatibility with the European Convention on Human Rights, as the Government acted unlawfully, abusing powers given by Parliament. The requirement to assess if the Investigatory Powers Act has found a balance between privacy and intrusion of information. Orwell explained through 1984 that he was concerned that the Government was becoming a dystopian surveillance state, as the balance between monitoring of individual information and maintaining privacy rights needs to be proportional[8].

Chapter three will explain the timeframe where legislation has been selected, and then reformed, specifically after the Regulation of the Investigatory Powers Act 2000[9] to include; the Anti-Terrorism, Crime, and Security Act 2001[10], the Prevention of Terrorism Act 2005[11], and the Regulation of Investigatory Powers Act 2016[12]. The need to reform legislation is due to the further acts of terrorism that have occurred over the last 17 years. The difference here, is that in some cases of terrorism justifies why privacy laws are broken, in comparison to when the Government is misusing its powers[13].

Another viewpoint is that with newer technological methods in the world, this creates newer ways for terrorism to occur. Although this questions why there is a need for privacy rights, as the Government are intruding upon personal sensitive information, all Acts being discussed only relate to invasion of privacy and intrusion when concerning serious crime and terrorism. Again, as newer terrorism is justified to break privacy laws, the difference the Government makes is that it uses powers presented for the purposes of terrorism, in non-terrorism related

[8] George Orwell, 'Nineteen Eighty-Four' (1st edn, Secker & Warburg 1949)
[9] Regulation of the Investigatory Powers Act 2000
[10] Anti-Terorrism, Crime and Security Act 2001
[11] Prevention of Terrorism Act 2005
[12] Regulation of the Investigatory Powers Act 2016
[13] The attacks on 9/11 or the London tube bombings.

cases. In previous cases and pieces of legislation the Government has misused its powers to investigate minor crimes against vulnerable individuals[14], showing that the state have felt that in the past it has been warranted to break privacy rights to monitor specific people. However, when being reviewed it has come to light that this has in fact broken individual privacy rights.

This dissertation will be reviewing how the Government extends its powers, and whether minor crimes are necessary to be monitored, as they normally fall out of the scope to warrant privacy rights to be intruded upon. Minor crimes should be excluded as they are not a strong enough justification to allow the privacy rights of the population to be waivered. As such, the UK Government have continuously amended, reformed, and updated legislation, to the creation of the current Investigatory Powers Act[15]. However, privacy and intrusion concerns have remained one of the biggest concerns, for whistle blowers, Members of Parliament and privacy activists. Edward Snowden reviewed the legislation to explain that "The UK has just legalised the most extreme surveillance in the history of western democracy. It goes further than many autocracies."[16] The media, and Snowden's comments sparked concern amongst the UK population, leading to 212,743 individuals signing a petition asking for the Investigatory Powers Act to be repealed. Although this may not seem a lot in comparison to the entire population of the UK, it is when considering that a large proportion of individuals were not aware that this was occurring due to modern day concerns.[17]

Another concern is that the Government has the authority to review its own agencies, rather than allow an independent organisation to review what actions are made. By having an independent organisation, rather than a Government agency to examine policy and cases

[14] Young children
[15] Investigatory Powers Act 2016
[16] Edward Snowden, '@Snowden' (Edward Snowden's Twitter Account, 17 November
[17] Brexit

allows the correct process of misuses of powers and correct legislative review. This allows the transparency needed for such an important issue, privacy rights, as it allows an organisation to be held accountable. Whereas, the Government abusing powers, then assess whether they have used them correctly could be considered an injustice or biased verdict. This would lead to the idea that the Government is able to self-assess and give bias judgements to its own decisions.

The Investigatory Powers Act has made it compulsory for Internet Service Providers to store an individual's information for 12 months, which can then be viewed by the Government and its agencies to assess whether there is a potential or current threat to society and national security. Information can be taken from: mobile phones, computers, cameras, and the internet in order to build up profiles of individuals and the threats they pose. The issue for this dissertation is whether the Government and its agencies have too much power, set out within the Investigatory Powers Act, which allows them to view personal sensitive data. The element of intrusion is based on the Government effectively branding all of society as potential threats, rather than only looking at known criminals or terrorists and known associates. Although this does enable a higher chance of deterring and countering threats, the fear that the UK Government is creating an 'Orwellian' style state where all individuals are spied on needs to be reviewed.

Research Question

The purpose of this dissertation is to establish whether the Investigatory Powers Act has balanced the argument between privacy and intrusion rights, or whether this has not been met, similarly to previous legislation. This will be established by looking at privacy and intrusion and how the Government has used its powers in the past, and then give an understanding on the new law. By investigating how critics and academics review privacy, combined with the study being conducted within this dissertation will be able to assist with understanding if the balance has been met. It is necessary to assess individual rights in a world that is becoming further modernized through technology, while also acknowledging the concern that fear is growing not only amongst the society in the United Kingdom, but all over the world. Information needs to be private, and the idea that criminal action could be causing this to be mistreated and used needs to be reassessed to ensure individuals personal sensitive information is being managed appropriately.

The Government intrudes upon privacy rights by monitoring individual information, one example being TalkTalk, who had information taken, due to a cyber-breach. Information such as; pornography, political and religious sites, health-focused websites, and pirate sites were all taken from TalkTalk's database showing the need for an individual's activity to be private. This is one of six of the largest databases in the UK[18], and if criminals can access these storage facilities, this could amount to mass information of individuals being misused, and the

[18] Claire Walker, 'Computer Law & Security Review' [2009] 25(4) Data retention in the UK: Pragmatic and proportionate, or a step too far? Pg 325-334

identification of individuals. Therefore, there is a need to establish a balance between privacy and intrusion[19] is necessary to protect individuals.

Research Objectives

Several objectives will be reviewed within this dissertation, as several further observations regarding the initial research question. This will be establishing whether there is a balanced: *keeping or showing a balance; in good proportions* or *taking everything into account; fairly judged or presented* between privacy and intrusion. The objectives aimed to be answered include whether:

- The Government has misused/abused powers given to collect information?
- Reform is needed within the current system in place to allow an independent organisation to have control over powers?
- Minor crimes should be monitored?

The need to view the definition of the term balanced will help understand what is being investigated. Therefore, intrusion and privacy rights need to find a balance where both are proportionate and not outweighing the other. Although the Government has given it powers to allow information to be stored, privacy has been breached in the past, and the concern that this will again reappear needs to be assessed to consider whether there is a need for reform.

By also assessing whether individuals find minor crimes need to be reviewed would be able to give clarity on the previous use of powers. The European Convention of Human Rights has

[19] Chris Johnston, 'TalkTalk customer data at risk after cyber-attack on company website' The Guardian [2015] https://www.theguardian.com/business/2015/oct/22/talktalk-customer-data-hackers-website-credit-card-details-attack accessed 03/06/17

currently deemed legislation to be unlawful, and if the Government is collecting information on a large scale, which allows the identification of individuals this will again be unlawful. This will be how intrusion and privacy play its part, as the potential abuse of powers is leading to the Government becoming a dystopian surveillance state, presented by Orwell is the need to look and assess the research question and objectives.

Privacy

This dissertation views privacy as: *the state of being free from the public attention – or the ability to act in a manner that will not be shared and noticed by society or the Government*[20]*.* The Human Rights Act define privacy as:[21] *the right to live your life with privacy, and without the interference by the state on matters of: sexuality, body, personal identity, relationships, and personal information*[22]. For the purposes of this dissertation both definitions are key, as both hold a different context socially and legally.

Privacy activists are concerned that individuals are having limited privacy rights. As an example, individuals who use social media have a mass amount of data collected on them[23]. With other half of individuals accessing the internet at least once monthly, the concern that the Government can monitor information of individuals, and that the balance of privacy and intrusion needs to be readdressed to ensure data is not misused. Originally, the creation of the camera sparked the first concern over "The Right to Privacy"[24] as society became fearful that the new technology of the time could capture someone's image and storing it.

[20] James Murray, Oxford Dictionary of English (Oxford University Press 2010)
[21] Human Rights Act 1998 Art 8
[22] Ibid
[23] https://www.emarketer.com/Article/More-Than-Half-of-UK-Population-Will-Log-on-Facebook-This-Year/1013627
[24] Warren, Brandeis, 'Harvard Law Review' [1890] 4(5) The Right To Privacy

A second example would be with the use of postcards, as a cheaper alternative to letters but with the knowledge that anything written could be read by another. Returning to the modern day, the concern now resides with mobile phones, computers, closed-circuit television[25] and the internet as the newest forms of technology that have information stored. Technologies have adapted and evolved so much in relation to terrorism that the Government continues to add more legislation to try to counter and deter new crime. The recent Investigatory Powers Act, has sparked concern that the privacy lives of individuals are going to be intruded upon by the Government by having data collected and used.

Returning to the research question and objectives, it is arguable that the Government should not have access to the amount of information they are currently able to monitor[26]. The data that can be viewed was intended for one person, and as such to take and store this information intrudes and violates privacy rights, especially when the Government, has in the past, misused powers, and its authority to target minor crimes. It is arguable that taking societies information to find criminal activity shows an unbalanced framework between individuals privacy rights and the intrusion used by the Government, showing the need to assess whether the system needs reforming.

The Anti-Terrorism, Crime, and Security Act 2001 is an example where the Government were considered to be unlawful when "suspected international terrorists"[27] were indefinitely detained within Belmarsh Prison[28] under Part 4 of the Act[29]. The European Court on Human Rights found the UK to be acting unlawfully, while derogating away from the Human Rights

[25] CCTV
[26] Echevarria, Morales et al, 'An E-government Interoperability Platform Supporting Personal Data Protection Regulations [2016] 19(2) CLEI Electronic Journal
[27] Anti-Terrorism, Crime and Security Act 2001, Pt IV, s21
[28] A and Others v. Secretary of State for the Home Department 2004 UKHL 56
[29] ACTSA

Act. This shows one example where the UK has been found to act unlawfully when concerning privacy rights, showing why it is necessary to investigate further privacy cases that regard newer technology – as it has yet to be completely reviewed.

The concern within this dissertation is how privacy's role is impacting in a society that is constantly being monitored. The argument that individual privacy rights are being intruded upon to attempt to protect the interests of the nation needs to be assessed to find the balance between the need to monitor information, while allowing individuals to have their privacy rights. Most people do not commit a serious criminal action, bringing into question why the Government justifies the storage and usage of information. Currently, this could be due to the fear element being portrayed by media officials[30]. As the trend of terrorism grows, the concern that harm will occur gives the Government some authority to allowing information to be used.

Within the legislation being used, all consider monitoring and investigating individuals proportionate when trying to counter/deter/prevent serious crime and terrorist actions. However, the legislation does not state this with minor crimes, as they may not be proportionate enough to intrude upon the privacy rights of individuals. One example, In Poole shows how legislative powers were used to assess whether children were in the correct school catchment area. This shows the Government violating the privacy rights of children/vulnerable individuals because of a school catchment area. This is not the purpose of legislation as this is not a serious crime, and as such has intruded the privacy lives of individuals, not warranting a proportionate justification for the invasion of privacy. The fear that does show is the Government's ability to access the privacy lives of individuals, and take

[30] Custers et al, 'Fear effects by the media' [2012] 171(4) European Journal of Pediatrics

information regardless of a need for a crime/terrorist action. Steve Saxby promotes the idea that privacy and individual's information being protected "is no longer adequate in a world where data flows across national boundaries".[31] The information age that society is in no longer regards the privacy rights of individuals. With the Government harvesting information on social media, with the ability to access messages and any information they require shows the need for privacy. As the internet especially has no boundaries between states, meaning information can be accessed not only by the UK Government, but anyone in the world.

With the rise of cyber security threats online, the need to keep data and information correctly stored ensures that there is not a breach in privacy. The National Health Service[32] is one example of how individual's information was attacked and intruded on, showing the need for more security and privacy rights when concerning the personal sensitive data of individuals. in contrast, an idea that the Government should have limited information of society springs to mind, as this could ensure the balance between privacy and intrusion is met. This is done by limiting Government access, which is what cyber-attackers are looking for, big databases harnessing mass information. By doing this, means that the privacy of individuals is intact, while removing the possibility of personal sensitive data, such as the National Health Services' database – as individuals hold their own information, rather than relying on the Government.

[31] Steve Saxby, 'Computer Law & Security Review' [2013] 29(1) The 2012 CLSR-LSPI seminar on privacy, data protection & cyber-security - Presented at the 7th international conference on Legal, Security and Privacy Issues in IT law (LSPI) October 2-4, 2012, Athens 4-12

[32] Chris Holder, 'Computer Law & Security Review' [2016] 32(4) Robotics and law: Key legal and regulatory implications of the robotics age (Part II of II) pg 557-576; Robert Booth, 'Cyber-Attack Set To Escalate As Working Week Begins, Experts Warn' The Guardian (2017) https://www.theguardian.com/technology/2017/may/14/cyber-attack-escalate-working-week-begins-experts-nhs-europol-warn accessed 18 May 2017

Intrusion

When discussing intrusion, *the act of deliberately putting oneself into a place or situation where one is unwelcomed or uninvited that affects the privacy of an individual.* Although the dictionary holds one perspective[33], the Human Rights Act, this includes the unnecessary intrusion into an individual's life[34]. By having both, again shows the legal and social aspects to assess how the Government is intruding upon society for the purposes of national security.

The Orwellian state is a theme that is continuously mentioned throughout the reading of articles and journals. The fear that Orwell presented in 1984, where the super state monitors all of society and invades the minds of individuals, carried out by the "thought police" who look for "thought crime" using two-way television screens. Although Orwell believed when writing that super states would begin in 1984, the idea that he may have been in the wrong time period, as 15 years later there is a concern amongst privacy activists[35] who feel their rights are being ignored. This shows that there a worry around the UK becoming like 1984, and the comparisons between privacy rights, although largely different – could become similar over the next few years if the Government fail to address privacy concerns.

Orwell's view was that "On one side there are civil liberties groups demanding increased privacy and transparency; on the other there are 'securocrats' and law enforcement spokesmen, under pressure to keep us safe and facing a bewildering array of security threats, insisting they need to monitor more of our online behaviour… The debate is lurching whether to opt for a dystopia state, where our every move is secretly monitored, recorded and

[33] James Murray, Oxford Dictionary of English (Oxford University Press 2010) https://www.google.co.uk/search?q=privacy&oq=privacy&aqs=chrome..69i57j69i61j69i65l2j69i61j0.1652j0j7&sourceid=chrome&ie=UTF-8#q=privacy+definition

[34] Human Rights Act Art 8

[35] Amnesty International

analysed, or a world where criminals are able to do what they like."[36] Both sides are inspired by fear, and as such most of the public find it difficult to establish technology[37], and find law enforcement fragmented and opaque. As such, intelligence can be harvested and distributed in ways found to be unlawful. This was originally shown in the Edward Snowden sagas, and due to the disclosure threats being deemed too specified, has been kept secret from society. Politicians have tried to cover this with the informed debate of "*unprecedented threats to our society*" and the "*snoopers charter*"[38].

MP's are questioning the Government on why certain agencies are allowed access to powers within the Investigatory Powers Act, as it is allowing access to a mass amount of data and an individual's privacy. Two examples being the Food Standards Agency and the Gambling Commission. MP's[39] have questioned why such power has been given to agencies and whether they need that power. This then raises concerns on who should be able to add and remove agencies who are able to use legislative power, and if the current agencies should be on the list, as privacy rights have been breached by some in the past. Poole council is an example of privacy continuously being intruded on[40].

When using Phones and the internet as an example, the initial thought is that both are being increasingly used in the world[41]. The amount of information that can be extracted and stored

---

[36] J Barlett, Orwell v Terrorists [2015]
[37] Castro & Mcquinn, 'The Privacy Panic Cycle: A Guide to Pulic Fears About New Technologies' [2015] Information Technology & Innovation Foundation
[38] Burgess, 'What is the IP Act and how will it affect you?' http://www.wired.co.uk/article/ip-bill-law-details-passed Accessed 12 June 2017
[39] David Davis; Tom Watson; Andy Burnham; Jenny Jones (few MPs questioning the powers of the Act)
[40] Astrup, 'RIPA Powers only used by Poole council twice since 2009 after spying outrage' [2016] http://www.bournemouthecho.co.uk/news/14183694.RIPA_powers_only_used_by_Poole_council_twice_since_2009_after_spying_outage/ Accessed 12 June
[41] Suhang et al, 'Impact of Excessive Mobile Phone Usage on Human' [2016], Human. J Comput Sci Syst Biol

from: texts, call history, browser history use, and social media[42] has amplified so much due to the use of data on the move and with the advancement of the information age showing that although the extraction methods have enlarged, the duration of use has also increased. This shows why the Government is using the information gathered, to deter crime and terrorism, due to the mass amount collected[43]. The Government have tried to ensure that privacy and intrusion is balanced, on the basis that national security is being maintained, while trying to keep individual privacy rights, and the correct approach when deterring these threats. However, the UK legislation that was previously in force was considered as; illegal, lacking proportionate review, and incompatible with the Human Rights Act[44] as minor crimes are being monitored. Therefore, the need to assess whether the Government is using its powers correctly, for serious crime and terrorism, instead of intruding upon rights is necessary to establish whether the balance has been met in new legislation.

Max Schrem is one example of data being stored and used, which the Government could potentially access[45]. The access rights they have could identify individuals, which has been proven in cases related to journalists[46] and whistle blowers shows that due to the amount of information available today, individuals are easily identifiable, which shows a big invasion of privacy rights. Schrem found 1000 pages of information about himself on one social media site which included; friend requests, searches, and deleted members on his account. This shows just how much information is collected about one individual on one site. When relating this back to intrusion and privacy rights, the idea that the Government is able to access one

[42] J Roberts et al, 'The Invisible addiction: Cell-Phone activities and addiction among male and female college students' [2014], Journal of Behavioural Addictions
[43] C Brown, 'Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice' [2015] International Journal of Cyber Criminology 9(1)
[44] Human Rights Act 1998
[45] Schrems v Data Protection Commissioner [2015] Case C-362/14
[46] D Brennan, 'Still a 'Safe' Harbor? – implications of Schrems v DPC' (7)5 Data Protection Ireland

of the largest data pools in the history of civilisation poses major privacy concerns, and that intruding upon an individual's life is made easily accessible[47].

With the Government being able to access information whenever they require it shows just why intrusion of information and an individual's private life needs to be assessed to see whether there can be a balance between both opposing sides. The record Schrem shows exactly why the need to find a balance between intrusion and privacy rights is a necessity today, as mass information is being collected and observed to try to counter crime. There is too much information that the Government can access, and identify one individual which breaks the right to privacy[48]. The Government does this by using legislative powers to find potential criminal behaviour, while also collecting data on individuals within society.

The need to review previous legislation and assess where the Government and its agencies have gone beyond the proportionate and necessary and intruded into the privacy rights of society is needed. This will show if there are problems within the Investigatory Powers Act, how they can be reformed, to find the appropriate balance between privacy and intrusion. This relates back to the research question as the need to establish an appropriate balance is needed to ensure privacy for individuals is maintained, while also allowing intrusion rights for the purposes of national security. By assessing whether there is too much data on individuals will show that the Government is using its powers to try to investigate individuals that may not be committing crimes[49].

---

[47] K Rawlinson, 'Snoopers' Charter? That's's the least of your worries' [2012] The Independent, http://www.independent.co.uk/life-style/gadgets-and-tech/news/snoopers-charter-thats-the-least-of-your-worries-7854798.html Accessed 12 June

[48] ibid

[49] Ibid

Investigatory Powers Act 2016

Chapter 4 will analyse the privacy and intrusion debate within the previous Acts needs to be reviewed to assess the abuse of power that has been shown already within the Anti-Terrorism, Crime, and Security Act. Further privacy legislation needs to be reviewed, to consider whether the Government is abusing powers, which can be shown in the history of powers being used. By assessing this by using historical evidence of previous legislative failings, will show whether the Investigatory Powers Act addresses privacy concerns, as the balance between privacy and intrusion was previously unbalanced. Privacy within previous Acts has been breached, and within this dissertation further examples will show where the Government has gone beyond the necessary, while arguing for an independent organisation to take over and control the storage of information and the intrusion when necessary to deter crime.

When looking at intrusion, the need to do this is for the purposes of serious crime and terrorism, which has been apparent since the Terrorism Act 2000. "interception of communications… and disclosure of data…, the use of covert human intelligence sources and the acquisition of… electronic data protected by encryptions or passwords… may be decrypted or accessed"[50] shows what forms of information the Government initially began taking. 17 years later the possibility that more could be taken to deter individuals portraying elements of "serious violence against a person… creating a serious risk to the safety of the public… or… to seriously interfere or severely disrupt an electronic system."[51] The Government base this on "reasonable grounds for suspecting"[52], giving its agencies the ability

[50] Regulation of investigatory Powers Act 2000
[51] Terrorism (United Nations Measures) Order 2009, Pt II
[52] Claire Macken, Counter-terrorism and the detention of suspected terrorists (1st edn, Routledge 2013)

to: spy, track, and deter any potential criminals. This causes privacy concerns as the Government also are able to review individual information, and if they assess whether someone is potentially going to commit a crime and they are wrong, the Government agencies then have intruded upon an individual on an error.

Therefore, the Investigatory Powers Act needs to be reviewed in the future by the Government if found that agencies are misusing the powers within the legislation. The idea originally of ensuring the protection of society is good, providing all individual's information is protected, private, and will not criminalise them for minor crimes when the Act should be deterring serious crime and terrorism. The argument that the 'greater good' could be viewed here as a justifiable means, however by collecting mass data allows individuals to hack into the system and use the information maliciously. The greater good allows the risk of personal sensitive data to be breached, in order to protect the state. It is difficult to establish which one is better because it has not been confirmed how many crimes are stopped daily by abusing the privacy rights of individuals. Minor crimes are one focus that should not be reviewed as legislation has always tried to look at serious crimes and acts that could affect the nation, set out by the Crown Prosecution Service.

By looking at evidence from the past, with critical views and the views from the public should give an interpretation into the way the Government can progress, and not continue to brand all of society as potential criminals, when only a small quantity of individuals are causing serious threats/acts of terrorism. This relates back to the research question as there has previously been a breach of privacy for individuals, meaning the Government and the legislation has too much power over society, and the potential need to reform to enable individual's to have the privacy rights they deserve.

2 – Literature Review

A literature review identifies, analyses, and evaluates work produced by researchers and scholars. For the purposes of this dissertation a multiple number of articles will be reviewed to show how a variety of researchers view privacy and intrusion in today's world, to then assess whether there is a fair balance between intrusion and privacy. If there is not a fair balance, the process of assessing researchers views and recommendations then evidences why there is a need to identify the balance of individual privacy rights and the intrusion of rights to show a perspective from authors who are experts within aspects of privacy law. This would then meet the research question and objectives to show the misuse of power in the Government and the possible reforms necessary to ensure that further abuse of power is prevented.

By looking at the aspects of privacy will also give further evidence to show that the balance between the right of privacy and whether the Government is being invasive towards personal sensitive information. The Government intrude information by extracting, and enhancing the knowledge it already has on its citizens. This will help evidence the previous and current issues within legislation, to provide an outcome to reform the balance of power between intrusion and privacy.

'Panic Stations: Surveillance in the UK'[53]

Julian Petley reviews online activity in relation to terrorism laws, to show the decisions the Government makes out of fear and ignorance. He does this by comparing 1984 to the current state of online activity being controlled by the state, and that any activity is being monitored.

[53] J Petley, 'Panic Stations: Surveillance in the UK' [2013] 42(1) From online activity to terrorism laws, the government continues to make decisions based on fear and ignorance argues Julian Petley

Petley discusses how the information age has made illegal activities such as paedophilia and terrorism more difficult, while also monitoring those not committing a crime. However, Petley goes further to explain that even newer technology has helped track individuals who are suspected of committing a crime.

The Snoopers' Charter was originally created before the Investigatory Powers Act, but did not become legislation. The disregard to Human Rights forced the Government at the time to abandon this, only to redraft the paper to become the Investigatory Powers Act. The legislation reviews "suspected terrorists, paedophiles or serious criminals". After disagreements within the coalition, the proposed Bill was redrafted to ensure that the interpretation of legislation made by police and prosecutors was reviewed, enabling the Investigatory Powers Bill to be enacted. Petley returns to the first terrorist legislation, The Terrorism Act 2000, explaining that it is an offence to collect or make a record of information likely to be used to a person committing or preparing an act of terrorism or to possess a document or record containing information of that kind. Petley reviews the downloading of the *Al Qaeda Training Manual* and even though in cases where the user was allowed to download this, for university or a theology based perspective, the police attempted to convict individuals for terrorism based offences.

This shows that although individuals have lost their right to privacy, by researching a manual that can be found "on the website of WH Smith"[54]. This demonstrates how easily it is to access information that the Government perceived to be for terrorist purposes. This shows the intrusion of individuals rights as the Government has invaded their personal life, looked at the information individuals were researching, and prosecuting them. The fact the

[54] Julian Petley, 'Panic Stations: Surveillance in the UK' [2013] 42(1) pg 70

Government are perceiving this as a potential criminal manual, yet allow individuals to buy this online brings forth the idea that the Government are not spending an effective amount of time reviewing what should be deemed as a crime or terrorist activity.

One example of this is in 2008 when Rizwan Sabir, a Master's student was arrested for downloading the manual, which was confirmed by his supervisors confirmed this, before being released 7 days later with no apology. The police continued to hold intelligence on Sabir, as he was convicted of a terrorist offence which was untrue. Due to; false imprisonment breaches, Human Rights violations, and data protection violations the police compensated Sabir £20,000. The violations Sabir received clearly shows an intrusion of an individual's private and academic life – while also showing how the Government have too much power, even in 2008.

Petley then reviews legislation that was previously drafted broadly and hastily, without proper attention to Human Rights. Petley does this by analysing individuals who have been criminalised for the first form of monitoring individuals, by looking at pictures that were taken and developed. One case involving the prosecution of Lawrence Chard, a photographer who took innocent pictures of his children in the family pool. Due to the police successfully prosecuting Chard, the magazine Amateur Photographer launched a campaign for common sense – aiming to help photographers that were being prosecuted around that time. A string of previous cases before 2000 emerged where parents took their innocent photo films of their children to pharmacies, only to be arrested for having "erotic posing" pictures of their children in the bath. Again, this was untrue and even though the term "erotic posing" was introduced to stop the kind of abuse, parents were still prosecuted. This shows how much power the Government had before 2000, and how the power they have remains in force, with the same

power and invasive abuse of legislation. The balance between privacy of an individual's private life and the intrusion that has happened is seriously unbalanced.

Petley clearly shows that individual's lives are intruded upon, before and during the period of time being reviewed, which damages an individual's private life and image as legislative powers given to the Government and its agencies are abused. Although this looks at The Terrorism Act 2000 – this clearly shows a violation of individuals Human Rights, which Petley then makes a worryingly comparison to Orwell's super state. This returns to the research question and confirms the concern regarding the balance between privacy and intrusion.

'UK Data Retention Regulations'[55]

Richard Jones' approach to reviewing data retention, the idea of storing information, by assessing how The Data Retention (EC Directive) Regulations 2007[56] have impacted the UK. By showing the purpose of the Directive, to enforce communications companies to store information for the police and security services. Agencies can then conduct "investigations, detection and prosecution of serious crime". Jones notes that due to this, retention of communication data is recognised as "valuable and important" as terrorist plots and serious crime have been deterred.

Jones discusses how the UK then reviews retention of data, specifically looking at mobile phones and the internet. The new legislation is applying only to the public providers of electronic communications' networks and services. Information asked to be retained includes calls (including unsuccessful attempts) and cell location for 12 months, with no maximum period for communications data to be retained. They are asked to remove the

[55] R Jones, 'UK data retention regulations' [2008], Computer Law & Security Report (2)4
[56] Statutory instrument 2007 No. 2199

data after one year, unless it is needed for billing purposes in the future. Although companies must enforce The Fifth Principle – the idea that once data is kept longer, information needs deleting, some companies need data to be stored for billing purposes. This means that although companies say they have to delete information after a year, this can in fact be longer as the information may still be necessary. Returning to the research question, this has implications on an individual as although their information is stored, this could be kept for longer than they once thought. This has privacy implications, more specifically when looking at potential cyber hacks. One problem clearly shown is there is no maximum restriction, and the company can keep information if they have an adequate reason for storing data is needed for further evidence.

Data is revealed to security agencies when needing a specific case, which is reviewed on the principles of necessity and proportionality. The need to assess these two factors is based on trying to keep individuals information private, rather than broadcasting the data they want to remain isolated. The Working Party of data protection established under Article 29 of the EU Directive have criticised the Directive as being too lax in relation of private communications data, which Jones compares to the "similarly jaundiced view of the UK implementation." This shows how Jones is making comparisons to the EU and UK's response to privacy protection rights, meaning the need to update and reform this should be considered to ensure the data received does not become invaded and abused against. When relaying this back to the research question, this is a similar balance that needs to be assessed. The argument Jones makes is whether storing and using data is proportional to the crimes being committed, relating back to the research objective of whether this should be for serious crime and terrorism, or minor crimes. As a previous example, Poole was spied on for littering and dog-fouling. This brings forth what is proportional and necessary for

deterring terrorism and serious crime, and to some this would be deemed as disproportionate. Therefore, Jones' article relates to the need for privacy rights, in a world where anything is monitored, without justification.

'Snoopers' Charter? That's the least of your worries'[57]

This article reviews one case, Max Schrem, before looking into police powers, internet users and companies. Kevin Rawlinson uses these combinations to analyse how data communication is affecting the UK Government, while showing several examples of how cyber hacking is influencing the need for new legislation. This relates back to the research question as this will indicate how intrusion affects society's perspective, while also showing the need for privacy rights and individuals to have their own information, rather than the Government having sensitive data.

Schrem has already been discussed, however he reports that "the scary thing was, with a simple 'Ctrl+F' search function on the computer, I could search for terms and key words. I found it was possible to build up a picture of who I am, what I like, who I might vote for." This shows how a company can invade the rights of individuals for the purposes of marketing and building up a personal profile, especially on social media. There appears to be a need for privacy rights against a company, but the need to assess whether the Government having access to this is what needs to be reviewed.

Rawlinson then looks at societies and companies legitimate and illegitimate uses against internet users. Two examples used include Google and Facebook that "feed off the data their users give them." This is used for marketing, by accessing what individuals have been

[57] K Rawlinson, 'Snoopers' Charter? That's's the least of your worries' [2012] The Independent, http://www.independent.co.uk/life-style/gadgets-and-tech/news/snoopers-charter-thats-the-least-of-your-worries-7854798.html Accessed 12 June

searching for, which then is tailored to their requirements for a specific advertisement. Another form of using data includes cookies, which creates an online map of where users have been. This tracks individuals through their Internet Protocol address, which gives an indication on the user's location. This relates back to the research question as the power companies such as Google and Facebook have the ability to record individual's information, which can then be accessed by the Government. This relays back to how much power the Government currently has on companies and individuals, with the intention to gain access.

As an example, Google has "one of the highest-profile sites when it comes to data collection" due to the "serendipity engine" that is being created. This is made by individual's information being tailored specifically to the needs of the user. However, this needs personal data which is found through social media or marketing online. James Lyne, the director of technology strategy at Sophos explains that the services individuals show how information is "actually exposed" even when "speaking to a closed group of privileged friends". This relates back to the Government having too much power. If the companies are able to harness and mine data as easily as they currently do, then Governments can access all data through the legislation that has been implemented.

Google have also admitted inadvertently collecting sensitive personal data using software installed in cars. A further example by LinkedIn shows that 6.5 million passwords were leaked onto a hacker's forum, indicating the level of concern regarding individual's privacy rights, especially when coming to a social media site. This is because of the mass data able to mine, shown previously, while also considering that users will normally put personal sensitive information online about themselves. This could be; mother's maiden names, pets and their names, their date of birth, the university/school they go to, pages they are

interested in, email addresses and their friends. These are mostly secret questions when using an online site, and as Vicente Diaz explains, “once it gets this far, you have already lost control of your data.” Therefore, the need to have more individual privacy rights is necessary to ensure that further hacking, the very thing trying to be deterred, is stopped.

The Government having access to information that has just been presented poses privacy rights of a different magnitude. By allowing the Government to have access to personal sensitive social media sites that has a mass amount of information shows the need for further privacy rights. By allowing companies to mine data, while then giving the Government the authority and power to access this poses severe violations of an individual’s rights. Having reviewed whether the Government should have access to these rights shows how privacy is unbalanced against the intrusion rights Governmental agencies currently have.

‘Data Retention in the UK: Pragmatic and Proportionate, or a step too far?’[58]

This article, presented by Claire Walker discusses the Data Retention Act 2009, which had just become enacted into power. This was the first time Internet Service Providers’ had to retain data, relating to customers email and internet usage on a compulsory basis, as opposed to voluntarily. This caused protest within private lobbying due to the concern over a “Big Brother” society, which then lead to Walker questioning policy backgrounds, practical implications for service providers and weighing up the argument between privacy and human rights concerns put forward to the Government. The way Walker examines how the Government acts in accordance with EU Data Retention Directive and the UK approach to

[58] C Walker, ‘Data Retention in the UK: Pragmatic and Proportionate, or a step too far?’ [2009] Computer Law & Security Review (25)

the regime shows the impact the Government has made on privacy rights for individuals. This is further evidence by Government cases and new Bills before concluding.

Walker originally looks at how data retention in the UK has occurred, relating back to the idea that communications data for intelligence is mainly to counter terrorism purposes. This is shown within the Regulation of Investigatory Powers Act 2001, highlighting the distinction between data retention and data preservation, subject to law enforcement authorities. Walker suggestions if there was already legislation in place, the events of terrorism – such as 9/11 would never have happened, and have acted as a catalyst for legislation that has been hastily introduced. Legislation such as the Anti-Terrorism, Crime, and Security Act 2001 which was the voluntary framework regime for retention of information of the telephone, email and internet data. The framework was finalised within 2004, agreed by service providers which was individually negotiated, including the reimbursement of certain costs by the Government. Here, this shows that the Government previously did not have enough power, possibly due to the lack of knowledge of terrorism at that period of time. When comparing that to now, where individual information is retained and users can sometimes be identified shows the transition of limited power to arguably too much power.

Walker discusses who is subject to the new regulations at that time, indicating public communication providers would be responsible for making electronic communications accessible to agencies. The need to assess who is responsible is based on industry concerns over powers and who would be liable under ambiguous responsibility regulations. The outcome states that larger internet service providers would be, over communication service providers, with the aim for CSP's to have "incremental" approaches to storing data built on the Anti-Terrorism, Crime, and Security Act regime. This shows who has the power to retain

data and communicate this to Government agencies. Data that can be stored and given out include data related to identifying subscribers and users through electronic communications. Other methods include data for billing purposes and identifying the location of a user. This shows what the Government and its agencies can currently identify, showing the breach of privacy in regards to knowing what an individual's preferences are and their current location, sparking privacy concerns as users should not be identified or located. They need to remain anonymous, highlighting why the need to reiterate a balance between intrusion and privacy is necessary.

The Government has brought to attention some potential reports that is worth noting, based on retention period, costs, sanctions and access of communications under legislation. By looking at these agendas set out, will show the Governments perspective of the implications they are willing to go to, to ensure national security is protected. This shows the argument the Government is presented with, when concerning individual privacy rights or intruding upon those rights in order to protect society as whole.

The UK Regulations have imposed a flat 12 month storage of all data types, removing the previous provision of allowing the Home Secretary of being able to vary the retention period by notice. This shows that the Government have noticed how previous powers were too extreme, and they have refined this to make it fairer for privacy rights. The reimbursement of the amount spent to retain data, due to compliance with the Regulations, is conditional based on the notifications the Secretary of State's agreements in advance and with compliance within audits. This shows that the Government is using money to fund the storage of data of individuals, without consulting whether society as a whole wants this to

happen. Although this is for deterring serious crime and terrorism, individuals could argue that they are neither, and as such should not have their information stored.

The sanctions imposed on communication service providers that fail to comply face civil proceedings for an injunction of specific performance of a statutory duty, giving a compelling reason due to the risk of consequences when failing to assist in matters of national security and serious crime. Again, this shows the Government having too much power over companies to comply, when ultimately it should be mandatory. The idea that companies are forced to store and give data over to the Government, when requested gives the impression of an Orwellian state again. The safeguards set out prevent the misuse of communications data and ensure access to information is proportionate. This does not state the measures in place, or whether there is a necessity to access information, indicating that the Government and its agencies if they believe information is proportionate and warranted for the purposes of dealing with serious crime and terrorism. The safeguards also do not show where the Government has extended its power to look at minor crimes, such as Poole where children were monitored and minor crimes were watched, rather than the more important issues that are justifiably more proportionate.

Under Regulation 6, communication service providers must follow data protection principles to; ensure all data is equally secure and protected, with the same organisational measures (which includes accidental and unlawful destruction of data), enforce the idea that all data is subject to technical and organisational access through specially authorised personnel, and to ensure all data is destroyed to the end of use/ retention period of data. This shows that although the Government do have the power to access information, and have enforced the need for data retention, in reality it is difficult for access of information. This returns back to

the objectives of whether they have too much power, and if this is intruding the lives of individuals carelessly. Here the Government have limited access rights and how agents gain information, while also showing a need to protect society as whole, indicating that although they have too much power, this is restricted because of the processes put in place.

Access to communications data is restricted, designated by a telecommunications operator under the Regulation of Investigatory Powers Act to obtain and disclose information if they believe it is necessary and proportionate to counter terrorism and serious crime. This is based on a necessity test to "obtain… data if… necessary: (a) in the interests of national security; (b) for the purpose of preventing… crime or… disorder; (c) in the interests of the economic well-being of the UK; (d) in the interests of public safety; for the purpose of protecting public health; (f) for the purpose of assessing or collecting… tax, duty or levy or other imposition, contribution or charge payable to a government department; (g) for the purpose, in an emergency, of preventing death or injury or any damage a person's physical or mental health;… (h) for any other purpose (not falling within paragraphs (a) to (g)) which is specified for the purposes of this section by an order made by the secretary of state". This shows how the Government determines whether to access information. This does not show whether individuals follow the legislation or whether there is independent oversight. This returns back to the research question regarding the Government having too much power to be able to warrant using legislation that will invade the privacy rights of individuals.

Those able to access data include police, the Serious Organised Crime Agency, the Scottish Crime and Drug Enforcement Agency, HM Revenue and Customs and the intelligence services. Statutory instrument has added other departments within the central Government, which have limited powers to accessing data. This has caused controversy with

public and opposition concerns about the powers being compared to the “snooper’s charter”. The Government have responded to try to restrict the public authorities’ access further, by restricting which authorities can be granted within local authorities under the Regulation of the Investigatory Powers Act.

An authority must be able to balance “the extent of the intrusiveness of the interference with an individual’s right of respect for their private life against a specific benefit to the investigation or operation being undertaken by a relevant public authority in public interest” under the provisions of the Regulations of the Investigatory Powers Act. Although this code is not binding the courts will use this as a marker to establish whether authorities are being lawful and meeting the necessity and proportionality “thread” in order to make a successful application to acquire data. This refers back to the point of the dissertation, which questions whether the Government have too much power and if authorities are balancing privacy and intrusion. Walker shows that the authorities are trying to do this, to explain that accessing information is more difficult, but this does not necessarily mean data is private. This simply means the Government must jump through certain hopes in order to acquire what they desire. This shows that although the process of getting information has been reformed, the Government has still too much power as it can access the same amount, therefore the authorities have not found a balance.

The need for independent oversight is clear, as Walker continues to explain that the Interception of Communications Commissioner carries out inspections of relevant public authorities and reports annually to Parliament. This is to assess legal compliance, and whether accessing data is effective. The Investigatory Powers Tribunal provides a further safeguard by hearing complaints by individuals relating to the Regulation of Investigatory

Powers Act. Although this provides two organisations that are able to assess whether the Government are acting lawfully, through the publication of its findings. There is no clarity around how independent the organisations are, as they are still a branch within the Government Authorities, meaning the users of the Act are effectively reviewing themselves.

Vienna University have found some areas that need highlighting; internet access, internet emails, spam, unsuccessful call attempts and blurring communications data and content. The Implementation Group have said they would attempt to reach a pragmatic stance on these problems, while understanding that there is still lots of work to do in relation to the handover of data and the retention of data. When internet access, not all forms generate User ID, examples being wireless LAN hotspots and unauthenticated dial up connections. This is similar to emails that have different types of protocols and records when identifying personal information. This ultimately depends on whether parties are customers to Service Providers. It is unclear whether spam is retained too, as 60% of emails are spam. This relates back to whether there is a need to retain personal information, especially spam, which holds no value to a users' account. Call attempts within the context of webmail, are copied out of the Directive, yet hold no relation to Internet Service Providers.

The evidence from the Government, as Walker states reviews the: proportionality and value of using data retention, the evidence gained from the 12 month of data, and access of data under the Regulation of the Investigatory Powers Act regime. Walker then reviews the future UK policy to modernise the programme, the Communications Data Bill, and the latest proposals for decentralising data retention. This shows the opposing side to have data retention. Although understanding the need for privacy rights, this shows the initial reasons why the Government have approved data retention in the UK.

Walker finishes by discussing the future of UK policies, through the use of the modernisation of programmes, the Communications Data Bill, and a decentralised data retention system. As the 2009 Regulations begin to stabilize within the statue book, the Government acknowledges the inadequacies for law enforcement, by launching a consultation to try to reform the first outlines in May 2008, which then were published in April 2009. The first policy stand begins with the Interception Modernisation Programme, outlining a strategy in 2007-2008 to use "ground breaking technology to stay well ahead of the terrorists". The Government have explained this is a necessity, and discussed the idea of a black box on all electronic communication for the GCHQ to investigate individuals. The promotion of this was based on a lower cost than implementing Internet Service Providers, while also showing the best way to centralise a database of information on individuals. However, this is clearly a privacy breach that would be opposed because the Government would be able to monitor, store and use data of an individual at any point. This returns back to Poole, when individuals were monitored. It is similar in the sense that even those who have not committed a crime would be monitored.

The Communications Data Bill was discussed in 2008, with the intention to "allow communications data capabilities or the prevention and detection of crime and protection of national security to keep up with changing technology through providing for the collect and retention of such data, including data not required for the purposes of communication services providers". This was to begin the possibility of a centralised database, which has raised concerns from the press, while questioning Parliament. This was based on the worry that recording all UK citizens' mobile and internet records was "a step too far". The Open Rights Group highlighted that this would mark a change under the Directive "where the Government can watch everybody". The final version of the Bill appeared in 2009 before

being rejected. This clearly shows the privacy concerns raised by companies and the media, raising the question of why the Government allowed agencies to have so much power. This then explains that the powers between privacy and intrusion were not balanced, which gives some indication to the current powers agencies have.

The latest proposals Walker comments on finalises her article, explaining within the consultation document that "protecting the public in a changing communications environment" is necessary to deter terrorism and serious crime. The Government has suggested the legislation is limited in its effectiveness, and will continue to erode with the advancement of technology – meaning less communications will be meaningful to investigators. The Government have expressed that the centralization of data and the cost would be altered, meaning data will be fragmented and a reduced expenditure is met. This shows the Government altering its previous proposals to make the legislation user friendly, while ensuring service providers do not feel they are spending their money on systems to retain data. This relates back to the research question as the balance between privacy and intrusion is trying to be met by the Government. Therefore, previous legislation shows that intrusion of individuals privacy has occurred, which the Government is trying to amend in the future legislation.

Conclusion

The four articles reviewed discuss storage of information, communication access, and the legislation surrounding intrusion and the privacy rights of individuals. Each article took different approaches when analysing the balance of power, while also assessing whether the Government had too much power. From the evidence shown, clearly there is a divide between those legislating and the citizens of the UK, as both views on privacy and data

storage are different. Although the Government deems it acceptable to use privacy powers to ensure the nation is protected as a whole, it could be considered that some individuals believe it is an abuse of powers to use their information, especially is they know it is not relatable to terrorism, to be used. The idea here is that individuals are happy to have the nation monitored, but not their own information when they believe that are not committing criminal actions. To monitor and review their everyday lives could lead to the assumption that they are being branded as a criminal or terrorist.

The idea of Orwell's 1984 has been reiterated several times throughout the articles, showing the concern amongst the future of privacy rights, as it would appear the "big brother" state is becoming more apparent. The next step to discuss is how the research for this dissertation was conducted, to try to further prove that the use and storage of data is becoming a threat to individual's privacy rights. Although the Government have shown that this is to prevent serious crime and terrorism, the need to protect the personal sensitive data of individuals is still needed. By choosing to monitor society as a whole does not make intrusion of privacy rights justifiable.

This relates back to the research question as the privacy of individuals and the intrusion put upon them has been explored within the texts. Clearly privacy is an aspect of people's lives that they feel needs to be kept hidden, or secret away from the public's view. The intrusion aspect shows that this hidden unexplored feature is essentially being attacked, and it would be considered not only an abuse of Human Rights, but of privacy rights of an individual (ethically, rather than legally) to have their hidden features exposed. Although privacy and intrusion are different sides of the spectrum, both are incredibly similar in the sense that each are topics of discussion, which will have room for debate. Intrusion has the aspects of

the Government of protecting the nation, while also invading privacy rights, while an individual's privacy is something to an individual that protects them from the nation (to an extent). To break the privacy rights protects a person from terrorism, while also allowing the Government to intrude, use and to a certain extent brand members of society as a terrorist or criminal.

3 – Methodology

Privacy, intrusion and the Investigatory Powers Act needs to be analysed. One method is by asking participants within a study to consider their own viewpoint around privacy and the possibility that their information can be accessed. The Investigatory Powers Act will not be questioned directly as individuals will not know the legislative power within the Act. By asking questions[59] based on privacy and intrusion, will give an idea on their views, while also answering the research aims and objectives surrounding the Investigatory Powers Act without participants knowing legislation.

The three methodologies found particularly useful for this study are the socio-legal perspective[60], black letter law[61], and a historical analysis[62] to determine whether there is a balance between privacy and intrusion, while also questioning the Governments power. The three-combined offer both a quantitative[63] and qualitative[64] perspective on privacy and intrusion, with the aim to answer both research question and objectives. Each will be reviewed to show their relationship with privacy, intrusion, and the Investigatory Powers Act. The socio-legal perspective will be shown through the questionnaires that have been designed[65] to ask students at Canterbury Christ Church University their opinion on privacy and intrusion, while the black letter and historic approaches will be found throughout the use of previous legislation.

---

[59] K Meadows, 'So you want to do research? 5: Questionnaire design' [2003] British Journal of Community Nursing (8)12

[60] N MacCormick, 'Four Quadrants of Jurisprudence' [1994] Percriptive Formality and Normative Rationality: Essays in Honour of R S Summers 53-70

[61] M Salter, 'Writing Law Dissertations: An introduction and guide to the conduct of legal research' [2007]

[62] G Robert, 'Critical legal histories' [1984] Stanford Law Review 57

[63] D Collier, 'Qualitative versus Quantitative: What might this distinction mean?' [2003]

[64] J Sale, 'Revisiting the quantitative-qualitative debate: Implications for mixed-methods research' [2002]

[65] C Williams, 'Research Methods' [2007] Journal of Business & Economic Research (5)3

Historical Analysis

By looking at previous legislation will show where the Acts have been considered as: intrusive, unlawful, and incompatible with Convention Rights. As already shown, the Anti-Terrorism, Crime, and Security Act has been incompatible. This should show the privacy concerns around the Investigatory Powers Act, to consider whether this new law will be just as unlawful as its predecessors, or whether privacy rights have been rectified.

By using 2000-2017 as the timeframe, this will show how terrorism and the advancement of technology within law has adapted to change the viewpoint on intrusion and privacy of an individual. By beginning with the Anti-Terrorism, Crime, and Security Act, ending with the Investigatory Powers Act will show how that during the timeframe the Governments viewpoint on privacy has changed, resulting in an Orwellian and intrusive state that monitors everyone[66]. If a piece of legislation is found to be unlawful, incompatible, or intrusive then the need to assess what has happened when reforming the Act will show the progression and change in privacy and intrusion rights throughout the years.

This will conclude with a breakdown of the Investigatory Powers Act, while providing pros and cons of monitoring individuals to consider whether the Government abuses the powers given to itself. By then comparing this to the evidence shown within previous laws will give an impression whether the Government is considering the privacy lives of individuals, or whether this has been ignored for the purposes of collecting data and countering serious crime and terrorism. This will also show whether serious or minor crimes are reviewed, to show whether the Government is complying with its own laws, to show whether law enforcement have too much power, and instead to consider whether an independent

[66] J Wesley, 'American Educational History Journal' [2011] (38)1,2

organisation needs to take this sector away from public, and to an extent Government control.

Black Letter Law

By reviewing the legal implications of privacy and intrusion within cases and legislation will show where laws have misplaced the balance between intrusion and privacy rights. By reviewing the previous laws and Investigatory Powers Act will show whether there is an intrusion of privacy. The powers within the Act can then show where powers have been abused, which have intruded on individual rights. Black letter law is normally used within legal dissertations as the method is used to collaborate, describe, and use legal rules to offer a significant look on legal authority's commentary. This is because it refers to the basic standard elements/principles of laws which are free from reasonable dispute. As this dissertation refers to the privacy rights of individuals, which are being intruded upon – it is only reasonable to review legislation, and its failings known to Parliament, to help with the future progress of new legislation.

This will give clarity to the legislation used, while offering commentary on the significance and impact of authoritative legislative stances. By using case law, statutes and academic commentary will then show where cases have been affected by privacy, the legislation affecting privacy and how powers are used to intrude on individuals. By reviewing how other critics have viewed the laws/cases to see if they also follow the same pathway that legislation and cases have gone. This has been criticised, and agreed to in Chapter 3 by others within the literature reviews, however by using laws and Acts that surround privacy will question whether the balance of power has been misused by the Government.

Socio-Legal Perspective

By using the literature review to show that authors are concerned about the privacy of individuals in the UK will enhance the argument that more privacy rights are needed on phones and the internet. By then using the data found within the research study will give an impression on society's viewpoint regarding privacy and the debate of information being taken and used.

By using a socio-legal approach, the assessment between the law and society, will look out how laws impact empirical knowledge and understanding of how laws and legal proceedings are affecting the privacy rights of individuals[67]. When putting this into context of their privacy and the idea that this is intruded upon, the 100% feedback received within the research study gives a clear indication that members of society want to discuss their privacy and the idea that their information is being viewed – because it violates everyone's right to a private life. The need for a small section of society gives a clear impact on the statistics received[68] to show that privacy lives of individuals are being intruded upon, and individuals would prefer that this is used for terrorism and serious crime, while also having their data withheld from law enforcement. This is where striking the balance is most difficult, because individuals would like to be protected, while also believing they should not be monitored because they do not consider themselves as a threat to the nation.

[67] C Nyst, 'The right to privacy in the digital age' [2017] Journal of Human Rights Practice, 9(1) 104-118
[68] R Little, 'Journal of survey statistics and methodology' [2017] Oxford University Press (5)4

Study

The study conducted for the purposes of this dissertation was questionnaires given to law students within Canterbury Christ Church University. The data received reviewed participants views towards privacy, and the possibility of this being breached by allowing the Government to view their data, while analysing what they would allow the Government to store information on.

The need to assess students was due to the ease of accessing the students and their understanding of changes in law. Each student has a basic understanding of privacy legislation, due to the modules they study at Canterbury Christ Church University, while members of society may not understand legislation as easily. The public may also have been harder to source, as their answers may be deemed private and confidential, whereas the students used knew that the study was important to assess how they view personal sensitive information. In a continuously growing digital world, students understand the need for passwords, confidentiality and the threats that could appear online, which is precisely why they were used – because they know the technology.

The participants have the ability to assess what they believe is right, while understanding of legal implications. When combining this with the socio-legal perspective of being law students and members of society where the Government is taking their information, storing data, and then using should show an understanding and willingness to show what they believed to be intrusion of power by the Government.

The use of questionnaires was to ensure a direct answer was shown in the form of closed questions, which means students then have the choice to pick an answer they believe is most important. Although this limited the responses individuals could give, the quantitative

data will show how as a collective group the need for privacy rights is so necessary in today's world, where the idea that personal sensitive information can be taken has brought fear to individuals, shown within the statistics. Other questions within the study review the Governments power, and the possibility of another organisation having this power, instead of the Government. This will then directly relate to the Investigatory Powers Act that gives power to the Government and its agencies to deter crime. The idea that this may no longer be accepted within society could be the outcome of the results, which will then give a response to whether as a collective society they believe the balance of intrusion and privacy is met.

Interviews and focus groups were considered but not used within this study, as individual responses were needed to give focused responses, rather than allow results to be misconstrued or be deemed as bias[69]. The use of questionnaires allowed open and closed questions, with a quick response from participants and the ability to process and formulate the data to ensure the smallest period – allowing the data to be analysed as much as possible afterwards[70]. The qualitative data has also been discussed in terms of the literature review giving, which has given an interpretation to what authors believe to be intrusive and what needs to be private[71]. By using quantitative numerical data allows this study to have a triangulation methodology, by allowing; qualitative evidence from the literature reviews, which are combined with the black letter and historical stance from legislation, with a

[69] A Quelhas et al, 'Biases in questionnaire construction: how much do they influence the answers given?' [2011] Faculdade de medicina uniersidade do porto
[70] W Williams, 'A Sampler on sampling' [1978], Wiley (141)2
[71] P Wragg, 'Privacy and the emergent intrusion doctrine' [2015] Journal of Media Law (9)1

quantitative study from a socio-legal perspective – empowering the argument for more privacy rights[72].

As the Investigatory Powers Act is something individuals will not have read, the use of questionnaires makes it particularly easy to form a question for participants to answer, which will then be directly relevant to something they have not read. This is also applicable for intrusion and privacy aspects. However, each individual does have an idea of what they find intrusive and what should be considered as private, and it is interesting to analyse as a whole how they have reached the conclusion that will be shown within the findings of the study.

[72] A Acquisiti, 'What is Privacy Worth?' [2013] The Journal of Legal Studies (42)2

4 - Previous Legislation and the Investigatory Powers Act 2016

The purpose of this chapter is to show a historical position on how previous legislation has impacted and changed to become newer law. Legislation was changed/reformed due to the impact previous Acts had on individuals. When members of society are mistreated or their rights abused, a claim is made and as such the Government acts accordingly to ensure this is prevented in the future (through the form of review and reform)[73]. This means that legislation that was created originally is not necessarily correct or morally right, which is why the Government have to review and reform laws. By beginning at the Regulation of the Investigatory Powers Act[74], to then progress to the Investigatory Powers Act through only a few pieces of legislation will show where the Acts have had problems/discrepancies and how this has reformed to become the next piece of law. The Acts all have elements of privacy and intrusion rights that have been abused or misused, showing where the Government has previously failed, while also showing the need for reform. By analysing previous cases which involve the intrusion of privacy rights enhances the argument that the Government has been abusing the powers given, to then assess whether similar inconsistencies within the recent Investigatory Powers Act[75]. This will also give a perspective on whether using stored information is a positive or negative aspect, as examples will show that sometimes the Government agencies get cases wrong, and fail to recognise their own flaws. The chronological aspect is then clear as it shows the evolution of legislation involving privacy and intrusion, through the Acts specified to become the Investigatory Powers Act.

[73] T Weir, 'The Limits of Liability: Keeping the Floodgates Shut' [1999] 58(3) The Hague, London, Boston: Kluwer Law International
[74] Regulation of the Investigatory Powers Act 2000
[75] Investigatory Powers Act 2017

Regulation of the Investigatory Powers Act 2000

The Regulation of the Investigatory Powers Act[76] was originally introduced to regulate communications that needed to be intercepted. This was to account for the technological change within the UK, such as the growth of the internet and stronger encryption methods used. The purpose of the Act is to enable access to mass communication through surveillance for Internet Service Providers. This is done through facilities put in place, while an individual protects individual information and continue to monitor internet activity. The need for this Act to be rushed through Parliament was to help critics, who believed that terrorism, internet crime and paedophilia were occurring regularly.

Part I[77] allows the interception and collection of communications data. Secondly, Part II[78] allows the covert use of surveillance by authorities, regulated through intelligence techniques and safeguards for the public against unnecessary and disproportionate invasions of privacy. Lastly, Part III[79] allows the law enforcement agencies to require the disclosure of protected encrypted data, which includes encryption keys and passwords. With these three sections shows that the Government originally wanted to protect privacy rights, while also realising the need to invade individual's private lives to counter and deter serious crime and terrorism. However, it has been suggested that local authorities have been misusing and abusing these powers[80], even though the legislation has been trying to counter this – showing the need for the Government to readdress the imbalance of privacy and intrusion.

[76] Investigatory Powers Act 2017
[77] Investigatory Powers Act 2017 Pt 1
[78] Investigatory Powers Act 2017 Pt 2
[79] Investigatory Powers Act 2017 Pt 3
[80] The Report of the IOCCO Inquiry into the Use of Chapter 2 of Part 1 of the Regulation of Investigatory Powers Act (RIPA) to Identify Journalistic Sources [2015]; P Bernal, 'Data gathering, surveillance and human rights@ recasting the debate' [2016] Journal of Cyber Policy (1) 2

Abu Bakar Munir et al explained that the powers within RIPA[81] increased communication surveillance, while weakening data protection to ensure increased data sharing and profiling of individuals occurred. The purpose for the RIPA regulations was to intercept communications and the disclosure of data, while carrying out covert surveillance on electronically password protected data. This was done by ensuring Internet Service Providers accessed customer's communications secretly. This enabled a mass amount of surveillance, which would then continuously be monitored to prevent serious crime and terrorism.

The review committee of the Act explained that Parliament rushed through legislation due to the fear element of terrorism, with little debate to counter any further criminal actions. The lack of debate within Parliament over the powers that can be used have led to local authorities misusing its mechanisms for its own self gain. Rt Hon Keith Vaz has highlighted that there is a concern over "petty and vindictive" abuse and misuse of the Act, while Brian Binley has explained that local councils need to stop using the Act as a tool. Recent examples, such as the prosecution of Journalists within 'Plebgate' and Chris Huhne head led to the belief that the Act identifies individuals, breaking privacy laws, while also perverting the course of justice. This shows that the laws used within the UK that were created at the beginning of technological advancements broke privacy rights, and the balance between intrusions has not been met.

Critics[82] have speculated that the Regulation of the Investigatory Powers Act Regulations were excessive and a threat to civil liberties. Big Brother Watch published a report in 2010[83]

[81] Regulation of the Investigatory Powers Act 2000
[82] MP's Tom Watson, Jenny Jones, Shami Chakrabarti
[83] Big Brother Watch, 'The Grim RIPA' [2010] Cataloguing the ways in which local authorities have abused their cover surveillance powers

that reviewed the improper use of RIPA within local councils. This relates back to Poole Council[84] where privacy lives were intruded upon to check whether children were in the correct catchment areas. Jenny Paton is one case based on catchment areas, where she was wrongly suspected of lying about her address. Paton's telephone billing records were covertly assessed over a three-week period, while her car and children were also targeted to show the families movements. Although what they did is still considered legal, the privacy implications are clear to show that minors and citizens have been wrongly accused. This means the RIPA regulations needed to be reformed to meet the requirement within the Act, that serious crimes and terrorism acts needed to be watched, rather than a minor or wrongfully accused crime. This relates back to what should be private, and what is considered as intrusive, as it is clear in this specific case that the Government were invading the family's private lives.

Research suggests that 372 local authorities used the RIPA powers, and 8,575 cases were made in two years[85]. Each council carried out 11 operations each day for two years to monitor individuals. Within these cases, only 4.5% were prosecuted, with a majority concluding with the case being discontinued or finding that individuals were entirely innocent. This suggests that perhaps the need for local authorities to have powers to monitor individual's privacy lives is too extreme, due to the fact a small amount has a successful conviction. This also shows when assessing privacy rights and the intrusion involved within RIPA's powers, the balance between both have not been met, and instead individual's lives were previously abused and powers misused.

[84] Big Brother Watch, 'The Grim RIPA' [2010] Cataloguing the ways in which local authorities have abused their cover surveillance powers 47

[85] Big Brother Watch, 'The Grim RIPA' [2010] Cataloguing the ways in which local authorities have abused their cover surveillance powers 1

Other crimes being reviewed include: smoking bans, fly tipping and dog fouling. Although this does break the law, to compare this to terrorism and serious crime and justify the need to monitor individuals is difficult to comprehend[86]. Similarly, authorities have monitored their own employees to see whether they are; lying about their car parking, working at the correct times, assess sick pay, and spy on wardens who are employed to spot crime. Private sector companies do not have these powers, and for the public authorities to review its employees shows that the responsibility of powers has been broken. Within RIPA regulations entrusts users to be capable, and to have authorities misuse these controls in the context of employment disputes is concerning.

The Government have argued that by using RIPA powers will catch someone doing something but fails to address the type of society it wants citizens to belong within[87]. Although by using powers allows crime and disorder to be met, this is considered as disproportionate and illiberal as intrusive powers are used by the council, which seem unnecessary for the goal the Government wishes to achieve. Another argument would be that even when investigations into individuals are warranted, the surveillance methods used today are unnecessary – and that there is a simpler approach when reviewing individuals, such as asking. A final thought would be that some councils have managed without the powers, and instead of covertly intruding upon individuals privacy lives, they are overtly told that tape recordings will be made. This shows that although this still is intrusive, individuals are notified and informed that after several letters regarding an issue, then they will be monitored by councils. This questions whether it is right to use surveillance methods on

[86] Big Brother Watch, 'The Grim RIPA' [2010] Cataloguing the ways in which local authorities have abused their cover surveillance powers
[87] Big Brother Watch, "A Legacy of suspicion: How RIPA has been used by local authorities and public bodies" [2012]

individuals covertly, when Councils like Bradford – who use overt methods, gain a proportional outcome while protecting the privacy rights of individuals.

Proposals were made for RIPA, to try to balance the privacy and intrusion aspects. Firstly, the report suggested that no Council should have the powers within the Act, explaining that if alleged wrongdoing is serious enough then covert surveillance should be used by the police. This would be in cases of serious crime and terrorism, rather than dog fouling or littering. It is clear here that powers have been misused, and that Councils use them purely for because they are there. This is violating the privacy lives of individuals, for crimes that do not warrant a good enough explanation for abuses into the lives of citizens. The second proposal, failing removing powers is to permit RIPA powers with a warrant obtained by the Magistrates' Court for serious crimes only. This would allow powers to be used proportionally and reasonably in order to protect individuals, and their privacy rights. The problem here is that Councils have been told numerously to stop using RIPA powers but continue to do so. Finally, victims being monitored should be notified if found innocent, to explain why they were being watched. This would change the culture around oppressive powers, as those using such extreme methods had to also be held accountable to the victims being monitored.

Anti-Terrorism, Crime, and Security Act 2001

The Anti-Terrorism, Crime, and Security Act 2001[88] was introduced as an emergency step following the terrorist attacks on the World Trade Centre, September 11th 2001[89]. The aim

[88] Anti-Terrorism, Crime, and Security Act 2001

[89] D Lyon, 'Technology vs terrorism: circuits of city surveillance since September 11th' [2003] International Journal of Urban and Regional Research (27)3

was for the Government to implement this to try to combat any immediate threat the UK could face at that specific time. The Act was highly criticised due to the speed and lack of parliamentary review, which led to its initial review in 2002[90]. The need for this to be assessed was because of the intrusion on individual's privacy and liberty, as the powers set out within the Act allowed the Government to extensively review phone, internet and billing information. The 2002 report[91] has made various comments regarding the threat to privacy lives, and the intrusion innocent individuals have on their lifestyle when the justification to counter terrorism, by using their data, is not clear.

The Terrorism Order 2006 and 2009

The Terrorism Order[92], replaces the 2006 order[93] that was deemed to be a threat to rights, explains that 'terrorism' "is the use or threat or Action to influence the government to intimidate the public"[94] and "to use or threat to advance a political, religious, racial or ideological cause"[95]. These uses or threats can be defined as "serious violence against a person… involving serious damage to property… endangering a person's life… creating a serious risk to the safety of the public… or… to seriously interfere or severely disrupt an electronic system"[96]. Actions referred to within the Act also include explosives[97], used as a threat or Action as mentioned above as a threat to the state. The Treasury must be made aware of any relevant person or suspect in association with terrorism, who has committed an offence or is a restricted person[98]. The institution informing the state must make the

[90] Privy Counsellor Review Committee, 'Anti-terrorism, Crime and Security Act 2001 Review: Report' [2003]
[91] Privy Counsellor Review Committee, 'Anti-terrorism, Crime and Security Act 2001 Review: Report' [2003]
[92] Terrorism (United Nations Measures) Order 2009
[93] Terrorism (United Nations Measures) Order 2006
[94] Terrorism (United Nations Measures) Order 2009, Pt I
[95] Terrorism (United Nations Measures) Order 2009, Pt I
[96] Terrorism (United Nations Measures) Order 2009, Pt II
[97] Terrorism (United Nations Measures) Order 2009, Pt II
[98] Terrorism (United Nations Measures) Order 2009, Pt II

Treasury aware of information based on the suspicion[99], the person, the nature and quantity of any resources held for the relevant person for up to five years to relevant direction being given[100]. The term "reasonable grounds for suspecting"[101] is also difficult to interpret as it could be direct or indirect, acting alone or on behalf of somebody and designations imparts onerous regime on those selected. Only a designated person may deal with funds or resources belonging or owned by a person referred to within the 2006 order[102], unless under licence granted by the Treasury. In one key case where the Treasury acted on these issues was with regards to Al-Qaida, Usama bin Laden, the Taliban and other individuals, who had a list of criteria to ensure that on "reasonable grounds for suspecting" that a person or group of people were terrorists. The issues however within HM Treasury v A[103] was whether the Treasury or Executive, were empowered by the Act to allow introductions of terrorism orders or Al-Qaida orders by the Order in Council[104]. The contention of orders was ultra vires on three grounds; one being they passed into effect without parliamentary scrutiny, second the lack of legal certainty and proportionality, and lastly that there was no procedure available to allow any challenge. From a fundamental rights perspective, the orders were incompatible with Article 8(13)[105] and Article 1 of Protocol 1(14)[106] of the ECHR.

[99] Terrorism (United Nations Measures) Order 2009, Pt IV
[100] Terrorism (United Nations Measures) Order 2009, Pt IV
[101] Claire Macken, Counter-terrorism and the detention of suspected terrorists (1st edn, Routledge 2013)
[102] Terrorism (United Nations Measures) Order 2006
[103] HM Treasury v Ahmed 2010] UKSC 2
[104] HM Treasury v Ahmed [2010] UKSC 2; Joe Stevens, 'Journal of Terrorism Research' [2012] 3(2) Implementing 'targeted' UN Sanctions in the UK: Is Freezing of Terrorist Assets Giving Fundamental Rights the Cold Shoulder?' pg 1-10
[105] Human Rights Act 1998, Art 8
[106] Human Rights Act 1998, Art 1 Protocol 1

The Counter Terrorism Act 2008

The Counter Terrorism Act[107] was passed to increase police powers for countering terrorism. The main sections that need to be noted are; longer terrorism sentences, registering and monitoring those convicted for terrorism related offences, changes to rules surrounding the use of intercepting evidence, powers to seize the assets of convicted terrorists and the removal of documents from a property search to decide whether they need to be legally seized as part of an investigation. The 42-day terrorist detention without charge order was abandoned, which was previously 90 days, due to a single vote[108]. Although this was discussed and voted on heavily, the government believed that a Counter-Terrorism (Temporary Provisions) Bill[109] should be drafted to ensure any other form of terrorism that suddenly arose could be countered with this specific bill if needed in an emergency.

Draft Data Communications Bill 2012/The Snoopers' Charter

The bill was created to ensure communications data was obtained by public authorities. The bill replaced parts of RIPA[110], ACTSA[111] and the Data Retention Regulations 2009[112]. This was proposed by the Home Secretary in 2012[113], and required Internet Service Providers and phone companies to hold records of all its users Internet history, social media, emails, voice calls, gaming history and messaging history to be stored with the service providers for 12 months. The bill was expected to be brought into legislation by 2014, but the former Deputy Prime Minister[114] withdrew support in 2013, forcing his party to block the legislation from

[107] Counter Terrorism Act 2008
[108] Counter Terrorism Act 2008
[109] Counter-Terrorism (Temporary Provisions) Bill 2008
[110] Regulation of Investigatory Powers Act 2000
[111] Anti-Terrorism Crime and Security Act 2001
[112] Data Retention (EC Directive) Regulations 2009
[113] Theresa May, MP
[114] Nick Clegg, Deputy Prime Minister

being reintroduced. The government then reintroduced the bill in the form of the Draft Investigatory Powers Bill[115], but with more limited powers and additional oversight.

RIPA[116], being the original bill, gave Data Collection powers to Communication Service Providers[117] to collect and retain information about their uses, while under the Draft Communication bill allowed any organisation to interact with users and produce or transmit electronic communication to collect and retain information, regardless of its relevance to the business/user. The technique used is known as Deep Packet Inspection, which are the black boxes discussed later, to probe when Communication Service Providers refuse to submit data. The bill discussed later within this chapter will try to enforce CSP and ISP's to store data and give data when the government requires it. The filtering arrangements have not completely been discussed, allowing honeypots for casual hackers, blackmailers, criminals and foreign states to seize giant databases due to the broadly worded and poorly drafted provisions.

The powers within the Bill were to change the way institutions accessed communications traffic data, under the Interception Modernisation Programme. The programme was a government initiative to extend the capabilities of lawful interception and storage of communications data, eventually leading to storing details of all UK communications data in a central database, similar to the National Security Agency Call Database. The main principles were to collect data on calls, emails, chatroom discussions and web-browsing history habits, requiring the insertion of black box probes into the UK's compute and telephone networks. Huhne explained that the "Orwellian plans" to view private

[115] Investigatory Powers Bill 2016
[116] Regulation of Investigatory Powers Act 2000
[117] CSP's

communications were “deeply worrying”[118]. The Home Secretary[119] in 2009 suggested that there were no plans to create a “single central store”[120] for data, suggesting that the government’s stance on keeping all data together had changed. The current plans are to involve Internet Service Providers to spend £2 billion on deep packet inspection equipment within their own networks, forcing them to work with the government to perform the cross-correlation and profiling their users’ behaviour themselves, meaning the original programme is still achieving its goals, but not in the original plans suggested.

This was not a firm legislative format and was opposed by the opposition. The coalition agreement ended storing email and internet data without good reason. The coalition also reviewed the problems with the Interception Modernisation Programme and the access to communication and have since created the Communications Capabilities Development Programme as a modified and up to date format of the Interception Modernisation Programme.

The Communications Capabilities Development Programme[121] has extended the lawful interception and storage of communications data, involving logging of every phone call, email, text message between all inhabitants in the UK, but would not keep records of emails, and is trying to extend the realms of telecommunications to log communications within social media networking platforms such as Twitter and Facebook. The aims were to pursue terrorist attacks, prevent people becoming terrorists or supporting terrorism, strengthening protection against a terrorist attack and prepare to mitigate the impact of a

[118] http://news.bbc.co.uk/1/hi/uk_politics/7671046.stm
[119] Jaqui Smith, MP
[120] Alan Travis, ‘Government wants phone and internet providers to track users’ The Guardian [2009] https://www.theguardian.com/uk/2009/apr/27/home-office-superdatabase-email-phones accessed 03/06/17
[121] CCPD

terrorist attack. The CONTEST[122] document has stated that a change in privacy laws are needed for the CCPD to be completely legal.

Several issues with these programmes, which causes controversy when applying legislation, such as the Draft Communications Data Bill[123], as it allows "investigators the potential to identify other forensic opportunities, identify witnesses and premises of evidential interest"[124], meaning government officials could use this as a "fishing expedition"[125] if the cost was to be lowered. Secondly, to give government agencies power to review communications traffic data needs oversight of data collection and processing. This means control of data will be difficult without an external company auditing the way data is gathered, and viewing the operations that RIPA[126] and the Data Protection Act[127] comply with. It also further brings whether the auditors, people using the powers, or any other person involved are the right people to manage all private information. It is unclear how data is regulated, suggestions of a judge-given warrant or senior official would be enough to review basic data sessions. The RIPA[128] powers have already been abused by government agencies, so to give new legislation and powers could be a possible bad thing, as once again is the person using these powers the right person, or should it be another. A fourth consequence would be the cost, of an excess of £1 billion after Communication Service Providers[129] and Internet Service Providers implement and install systems to conform to

[122] HMGovernment, 'CONTEST: The United Kingdom's Strategy for Countering Terrorism' [2011]
[123] Draft Data Communications Bill 2012
[124] Alan Travis, 'Snooper's Charter' to check texts and emails' The Guardian [2008] https://www.theguardian.com/uk/2008/aug/13/privacy.civilliberties accessed 03/06/17
[125] Open Rights Group, 'Communications Capabilities Development Programme' [2012], The Communications Capabilities Development Programme has now, as of May 2012 produced proposed legislation, the draft Communications Data Bill.
[126] Regulation of Investigatory Powers Act 2000
[127] Data Protection Act 1998
[128] Regulation of Investigatory Powers Act 2000
[129] Don't Spy On Us, 'Snoopers' Charter Could Hit Police Forces with £1 Billion Bill' [2016] Proposals to collect the internet connection records (IRCs) of every UK Citizen could cost more than £1 billion. There costs, which

government legislation. The feasibility and cost was made clear in 2009, and reiterated in 2010[130], by the Information Commissioner that it was too much, and was abandoned the estimate and refused to put a price on the programmes.

Personal data is another big problem as there are problems with cyberterrorists, who go online to destroy systems and mechanisms, and "insider threats"[131] who are either corrupt or incompetent, putting the risk of vulnerable people such as those fleeing abusive relationships at a greater risk of harm. The government had commented that highly confidential details will be safe, however with such a huge system, if an "insider threats"[132] was to pursue and take information, they would be able to. EU Law then has its final say to discuss that privacy is a Human Right and that the programmes would be violating these protections due to the proposed collection and storage of data, meaning the Communications Data Bill[133] is incompatible with EU law, regardless of the Home Office assuring that the programmes and bill would be compatible. The Article 29 Working Party issued a report in July 2010 to[134] question if EU Law should stop member states from issuing further legislation that went above and beyond the current EU data retention laws[135], and that data retention period should be shorter than the suggested 24 months.

Returning to the legislation, it is clear with the concerns stated above that the law could never could deal with the huge power, invasion of privacy, less encryption, the cyber risks,

---

would fall to the Home Office, could be the equivalent cost of employing 3,000 full-time police officers at a time of office cuts. https://www.dontspyonus.org.uk/blog/2016/03/30/%E2%80%98snoopers%E2%80%99-charter%E2%80%99-could-hit-police-forces-with-%C2%A31-billion-bill/ accessed 03/06/17

[130] Rt Hon Sir Paulk Kennedy, 'Report of the Interception of Communications Commissioner for 2009' [2009]

[131] National Crime Agency, 'National Cyber Security Centre' [2016/2017] The cyber threat to UK business

[132] National Crime Agency, 'National Cyber Security Centre' [2016/2017] The cyber threat to UK business

[133] Draft Data Communications Bill 2012

[134] Article 29 Data Protection Working Party, 'Opinion 3/2010 on the principle of accountability' [2010] 00062/10/EN WP 173

[135] Data Retention Directive 2006/24/EC

costs, burden of ISP's and CPS's would make the bill difficult to bring into power. The need to review this bill is so that the public do not lose their privacy it is the most important aspect within these recommendations suggested to the government. Alongside this, to then scrap the idea and move onto the Draft Investigatory Powers Bill[136], which gives more power and more privacy rights seems problematic and unlikely.

Data Retention and the Investigatory Powers Act 2014

The Data Retention and Investigatory Powers Act[137] was enacted in response to a declaration of invalidity made by the COJ regarding the retention of certain communications data, which has now amended the 2000 Act[138]. Powers for retention of communication now belong with the Secretary of State who is to issue a retention notice to public telecommunications operators to retain relevant communications data if necessary and proportionate for the integrity, security and protection of data. This must be kept for 12 months, and cannot be exceeded, as stated within the ACTSA[139]. The relevant communications can be regarded as any telephony data stored in the UK or any internet data logged within the UK, meaning that any form of threat to national security could compromise an individual's rights if the state deems it necessary and proportionate with the Act. When considering how the UK spied on those families in Poole, it questions whether this Act is also being followed by the state, and if so, by how much.

The Investigatory Powers Act 2016

[136] Draft Investigatory Powers Bill 2016
[137] Data Retention and Investigatory Powers Act 2014
[138] Regulation of Investigatory Powers Act 2000
[139] Ibid (n 8)

Previous legislation therefore has created the Investigatory Powers Act[140] which has become one of the most sweeping surveillance powers in the western world. The Act has three main roles; to analyse communications data to view who is in exchange with individuals and when, but not the content within the documents. Secondly, to intercept data to contain the actual content in messages, secret recordings of calls and to obtain words in an email. Lastly, the third power allows Government agencies to gather any type of online communication to deter serious crime and terrorism to protect the security of the nation.

The need for this act is due to "modern communications… used by the unscrupulous… purposes ranging from cyber-attack, terrorism and espionage to fraud, kidnap and child sexual exploitation."[141] Due to constitutional, technological and issues of Human Rights, the Chair on Human Rights analysed this to explain that "The Bill provides a clear and transparent basis for powers already in use by the security and intelligence services, but there need to be further safeguards. Protection for MP communications from unjustified interference is vital, as it is for confidential communications between lawyers and clients, and for journalists' sources, the Bill must provide tougher safeguards to ensure that the Government cannot abuse its powers to undermine Parliament's ability to hold the Government to account."[142] The Act allows a range of Government authorities to have access to internet connection records without a warrant, raising issues on who can see individual's information.

[140] Investigatory Powers Act 2016

[141] David Anderson, 'Surveillance Powers: New Law Needed, Says Terror Watchdog' BBC News (2015) http://www.bbc.co.uk/news/uk-33092894 accessed 19 May 2017; David Anderson, 'A Question of Trust Report of the Investigatory Powers Review' June 2015, https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Web-Accessible1.pdf accessed 19 May 2017

[142] Harriet Harman, Joint Committee on Human Rights Chair; Legislative Scrutiny: Investigatory Powers Bill First Report of Session [2016-2017]

A legal challenge was made demanding the law be repealed as over 200,000 signatures[143] voted against the act[144], forcing Parliament to debate the Act. The issue was that internet providers are required to store customers' web history for 12 months and make the records accessible to Government agencies. Snowden, whistle blower on surveillance programmes explained the act was "the most extreme surveillance in the history of western democracy. It goes farther than many autocracies."[145] Snowden wrote this because the Act requires companies to break encryption, even though big companies such as Google, Apple and Facebook have argued this is "hazy"[146] and close to breaking privacy laws.

Technology companies are being forced to store information, meaning individuals are constantly being monitored, while their information is being stored in a massive bulk database. Security agencies have therefore, raised fears that companies' databases could be intercepted by hackers, which can potentially happen. This is due to a weakening in citizens' encryption activities to allow Government agencies to be able to intercept, decipher and monitor individual's information, set out in the Investigatory Powers Act[147]. With a lack of backlash over the Investigatory Powers Act[148], Internet Service Providers will be logging web browser information constantly. The main issue now is what is to stop an MP or a Government agency from using backdoor methods to find information on individuals. Plainly, the answer is clear, possibly a few years with an Investigatory Powers Commissioner delaying the powers

[143] Home Office, Government response to 'Repeal the new Surveillance laws (Investigatory Powers Act) (3rd May 2017) https://petition.parliament.uk/petitions/173199 accessed 19 May 2017

[144]

[145] Edward Snowden, '@Snowden' (Edward Snowden's Twitter Account, 17 November 2016) https://twitter.com/snowden/status/799371508808302596?lang=en accessed 19 May 2017

[146] James Titcomb, 'Petition to repeal new surveillance powers reaches 100,000 signatures' The Telegraph (2016) http://www.telegraph.co.uk/technology/2016/11/28/petition-repeal-uks-new-surveillance-powers-reaches-100000-signatures/ accessed 19 May 2017

[147] Investigatory Powers Act 2016

[148] Investigatory Powers Act 2016

if appealed, but ultimately none. What brings a scarier thought to mind is when will big companies such as Twitter, Facebook, Google, or Apple be forced to introduce backdoor procedures or be required to hand over user data.

Although the information being stored to look at is to check whether an individual is a threat to national security, all individual's information is now able to be reviewed with backdoor encryption methods, causing a contrast to data protection and privacy laws for the purposes of deterring terrorism. This was also done in previous laws, one specifically being Data Retention and Investigatory Powers Act[149] that was hurried through parliament and was incompatible with the Human Rights Act[150] and the European Union Charter of Fundamental Rights in R v Secretary of State for the Home Department[151]. The High Court found sections 1[152] and 2[153] of the Act to be unlawful, ordering the sections to be dis-applied, making it compatible with EU law. When considering this law, this has already been deemed illegal by the European Court of Justice because it allows "general and indiscriminate"[154] retention of electronic data. Liberty, a Human Rights campaigning group have commented explaining that although the country voted for 'Brexit' this should not impact the privacy and security of individuals. Although EU law will still be enforced for several years after Brexit, Parliament can then choose what needs to be removed. This means data protection or privacy rights could soon become extinct, allowing further surveillance laws to invade the rights of

[149] Data Retention and the Investigatory Powers Act 2014
[150] Human Rights Act 1998
[151] R v Secretary of State for the Home Department ex p David Davis MP, Tom Watson MP, Peter Brice and Geoffrey Lewis [2015] EWCA Civ 1185
[152] Data Retention and the Investigatory Powers Act 2014 s1
[153] Data Retention and the Investigatory Powers Act 2014 s2
[154] Madhumita Murgia, George Parker, Jim Brunsden, 'EU's highest court declares UK surveillance powers illegal' Financial Times (2016) https://www.ft.com/content/f847f522-c761-11e6-8f29-9445cac8966f accessed 19 May 2017

individuals further, showing the argument of the Orwellian state[155] being more apparent than ever to modern society.

Returning to the Investigatory Powers Act[156], there has been a public debate regarding the mass intrusive powers to agencies to gain targeted information as part of investigations[157]. The Home Office has insisted that this will be compatible with European Convention on Human Rights[158], however the Act has questioned to have issued with privacy rights. With pressure from politicians and judicial power, overseas organisations like Google and Facebook may have to release information annually, allowing "convenient silence… 500,000 times a year that communications data, such as call records, is tapped without any warrant at all". This bulk harvesting of data reviews traces left online, which has the power to "dissolve the very idea of privacy". The US a similar ideology has been cast with Obamas surveillance panel doubting the "presumption that extra data would beget extra security, and the federal courts have ruled against bulk collection." What is being questioned is if extra intelligence gains are worth the privacy lost[159] as David Anderson insists on a more "detailed operational case"[160] needs creating for surveillance in comparison to privacy and data protection.

---

[155] George Orwell, 'Nineteen Eighty-Four' (1st edn, Secker & Warburg 1949)
[156] Investigatory Powers Act 2016
[157] 'Computer Fraud & Security' [2017] 2017(1) Snoopers' Charter under attack pg 3; The Guardian, 'The Guardian View on the Draft Investigatory Powers Bill: Snooper's Charter 3.0' The Guardian (2015) https://www.theguardian.com/commentisfree/2015/nov/02/the-guardian-view-on-the-draft-investigatory-powers-bill-snoopers-charter-30 accessed 19 May 2017
[158] Home Office, 'Investigatory Powers Bill European Convention On Human Rights Memorandum' (2015) https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473763/European_Convention_on_Human_Rights_Memorandum.pdf accessed 19 May 2017
[159] 'Network Security' [2016] 2016(2) Impending Investigatory Powers Bill comes under fire pg 1-2; The Guardian, 'The Guardian View on the Draft Investigatory Powers Bill: Snooper's Charter 3.0' The Guardian (2015) https://www.theguardian.com/commentisfree/2015/nov/02/the-guardian-view-on-the-draft-investigatory-powers-bill-snoopers-charter-30 accessed 19 May 2017
[160] Terror Laws Watchdog, David Anderson

Conclusion

Surveillance is still today as apparent as it always has been. With global issues such as Russia[161], ISIS[162], North Korea[163] and the growing diplomatic problems between various states, not only is terrorism a threat but now a newer concept known as cyberterrorism has begun to infect the globe. The need for surveillance within the UK specifically is clear. With the recent London terror attacks[164] and attacks in Germany[165], the need to have alliances to combat and deter both types of terror threats are necessary. With the recent Investigatory Powers Act[166], this should be achieved with the powers granted to Government agencies to be able to investigate and store data, with the intention to be a better piece of legislation in comparison to its illegal and unlawful predecessors. The aim is to deter terrorism and serious crime, and although it is not possible to assess whether this is achieving its goals due to it only recently becoming legislation, the need to review this piece of legislation in the future is apparent.

The Government have tried to create this to deter terror and criminal actions through a surveillance method that is correct and lawful, and for the interest of the nation as a priority.

---

[161] Robert Mendick, 'Russian-Linked Cyber Gang Blamed For NHS Computer Hack Using Bug Stolen From US Spy Agency' The Telegraph (2017) http://www.telegraph.co.uk/news/2017/05/12/russian-linked-cyber-gang-shadow-brokers-blamed-nhs-computer/ accessed 19 May 2017

[162] 'The New Criterion' [2016] 34(5) Who speaks for Islam? Ph 1-4;Jason Burke, 'ISIS Celebration Over The London Attack Is A Dance of Defeat' The Guardian (2017) https://www.theguardian.com/uk-news/2017/mar/24/isis-celebration-over-the-london-attack-is-a-dance-of-defeat accessed 19 May 2017

[163] Andrew Griffin, 'NHS Cyber Attack: North Kora Is Behind Hack That Bought Chaos To Hospitals, Experts Claim' Independent (2017) http://www.independent.co.uk/news/uk/home-news/nhs-cyber-attack-hack-north-korea-who-behind-hospitals-hackers-lazarus-a7738026.html accessed 19 May 2017

[164] Helen Fenwick, 'International Review of Law, Computers & Technology [2011] 25(3) Counter-terror strategies, human rights and the roles of technology pg 107-115; Matt Dunham, 'London Attack: The Terrorist, The Bloody Aftermath And His Victims' The Telegraph (2017) http://www.telegraph.co.uk/news/2017/03/22/westminster-attack-pics/ accessed 19 May 2017

[165] Danny Boyle, Melanie Hall, 'Borussia Dortmund Explosions: Islamist Suspect Arrested Over Bus Bombs As Prosecutors Investigate 'Terrorist Link' The Telegraph (2017) http://www.telegraph.co.uk/news/2017/04/12/borussia-dortmund-bus-bombing-police-probe-islamist-letter-referring/ accessed 19 May 2017

[166] Investigatory Powers Act 2016

However, due to the previous laws the future question for another paper is to assess whether this act is legal, proportionate and compatible with the European Convention of Human Rights or, if the UK leave the EU, a British Human Rights. When these future issues arise in the form of future cases or enquiries, it is for the Government to act accordingly, and to show that although the Act is considered "the most extreme surveillance in the history of western democracy"[167], that there is a transparent, efficient, and lawful review system and procedure.

This clearly does impact privacy, data protection and personal sensitive information, invading the lives of individuals every day. The difference here is for society to assess whether this protects the interests of the nation, or whether there is a need to protect privacy rights. Necessity to ensure the rights of society over the insurance of individual rights has been analysed by critics, and it would appear there is a need for more privacy rights for individuals, especially "MP's, journalists, and trade unionists"[168]. With the rise of terrorist threats over the last decade, shown through the recent NHS attacks[169], it is clear the need to combat this to ensure protection of personal sensitive data is done. This could be done through not allowing data retention, which would therefore not allow Government agencies to review potential criminal and terrorist movements. An alternative is an opt out scheme by individuals with the right to be forgotten[170] by allowing the control of users' information to be removed online[171]. This could be difficult to remove everything, but removing social media information,

---

[167] Edward Snowden, '@Snowden' (Edward Snowden's Twitter Account, 17 November 2016) https://twitter.com/snowden/status/799371508808302596?lang=en accessed 19 May 2017

[168] Jenny Jones MP, Green Party, https://www.youtube.com/watch?v=3I3olv3u-fI&feature=youtu.be

[169] Christian Leuprecht, 'Government Information Quarterly' [2016] 33(2) Beyond the Castle Model of cyber-risk and cyber-security pg 2502-57; Denis Campbell, Haroon Siddique, 'Operations Cancelled As Hunt Accused Of Ignoring Cyber-Attack Warnings' The Guardian (2017) https://www.theguardian.com/technology/2017/may/15/warning-of-nhs-cyber-attack-was-not-acted-on-cybersecurity accessed 19 May 2017

[170] C-131/12 Google Spain SL, Googlge Inc v Agencia Española de Protección [2014] ECJ

[171] Said Shanin, 'Journalism & Mass Communication Quarterly' [2016] 93(2) Right to Be Forgotten: How National Identity, Political Orientation, and Capitalist Ideology Structured a Trans-Atlantic Debate on Information Access and Control pg 260-382

which arguably holds more information about a user as the individual is constantly using it by; updating your life, adding pictures, putting information on which could be considered personal. One method journalists are returning to using are pen and paper, as previous methods are less traceable than online, which is constantly surveying society. A final thought is for Government action to increase spending on security to ensure viruses, malware, and the software to ensure cyber terrorism does not become a greater threat.

When reviewing data protection, surveillance is becoming a greater threat due to two reasons; one being the lack of protection for individuals, and the second being the problem that with the recent surveillance laws, the backdoor encryption methods to gain access to individuals' information is vulnerable to hackers. The lack of privacy for personal information is an issue which could, arguably, be a threat to the fundamental rights of individuals' freedoms. The storage of data also needs to be upgraded to allow less threats to penetrate security as the big companies are being attacked, and personal sensitive data is being taken. Data mining and big data could therefore be argued on both sides as it is good to ensure that criminal actions are countered, but on the other side shows a lack of privacy and the possibility of hackers against big companies taking individuals data. Data protection clearly is inadequate in a world where data is constantly exchanged around the globe, and critics have made the comparison to Orwell's 1984[172].

[172] George Orwell, 'Nineteen Eighty-Four' (1st edn, Secker & Warburg 1949)

5 – Findings

This chapter reviews the study conducted at Canterbury Christ Church University in the form of questionnaires to law students. The study was conducted fairly and without bias, to gather effective results from individuals. The response rate received was 100%, as all individuals who were asked completed the questionnaire form and returned this on the same day. Only 30 individuals were asked as the students were in the middle of their revision in preparation for exams. The class should have been larger, but some students opted not to join the revision session.

The results found have been formulated on a table[173] and the 30 responses were electronically entered into each form to ensure anonymity was ensured. As some questions had individual's information, in regards to age and gender, the Data Protection Act warrants for the complete protection of participants. By electronically entering each individual's data, and ensuring all data was correct by re-checking allowed for individuals to remain completely anonymous in a high profile topic.

The data revealed in this dissertation is not the only pieces of information that can be extracted, and if at a later date this study was to be conducted again it may be interesting to see if any other data can be used. The statistics used will give an impression on how individuals feel regarding privacy, intrusion and their own personal sensitive information in a world where serious and minor crime, terrorism and the access of information is growing.

By using questionnaires allowed for the use of open and closed questions where available. The focus was primarily based on closed questions to be able to quantify the data into statistics, rather than allow participants to express what they truly believed as this would

[173] Appendix 1

have given room for interpretation on their answers which could allow bias. Focus groups and interviews were not used within this study as quantitative data was needed, rather than qualitative, but have been noted as something to consider in any following works on privacy and intrusion. The questions asked were:

1) How old are you?

2) Are you male or female?

3) Do you think the Government should be able to store information on individuals regarding you phone calls, messaging and internet history?

4) When the Government having information (regarding your phone calls, messaging and internet history) on individuals make you feel safer against terrorism?

5) Would the Government having information (regarding your phone calls, messaging and internet history) on individuals make you feel safer against serious crime, minor crimes or both?

6) Do you want your information (regarding your phone calls, messaging and internet history) to be stored and used by the Government for 12 months?

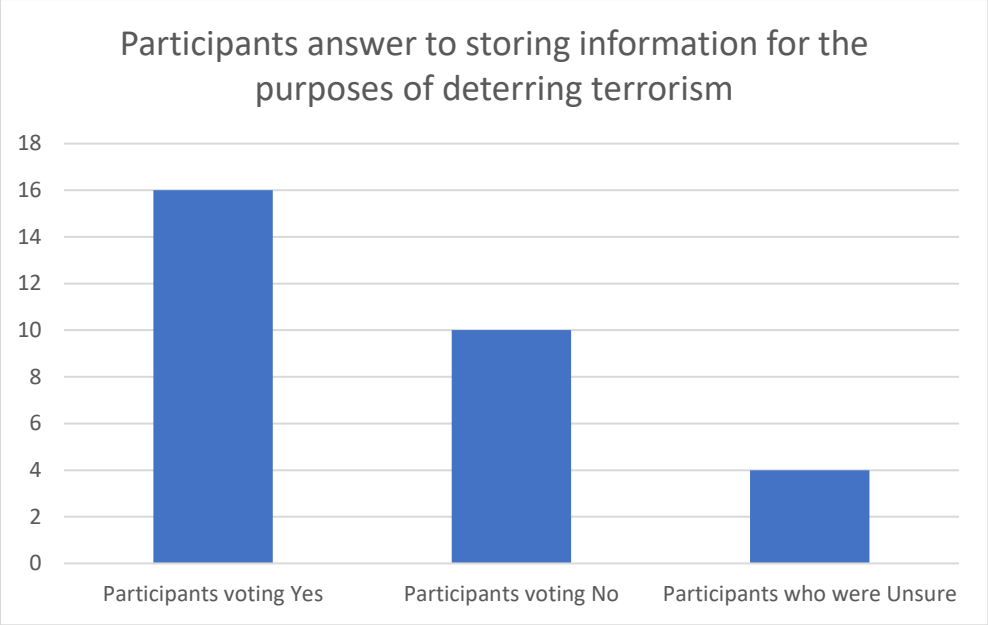
7) Do you think someone needs to be appointed to decide/ assess when public authorities should further investigate an individuals' data?

8) Who should this be?

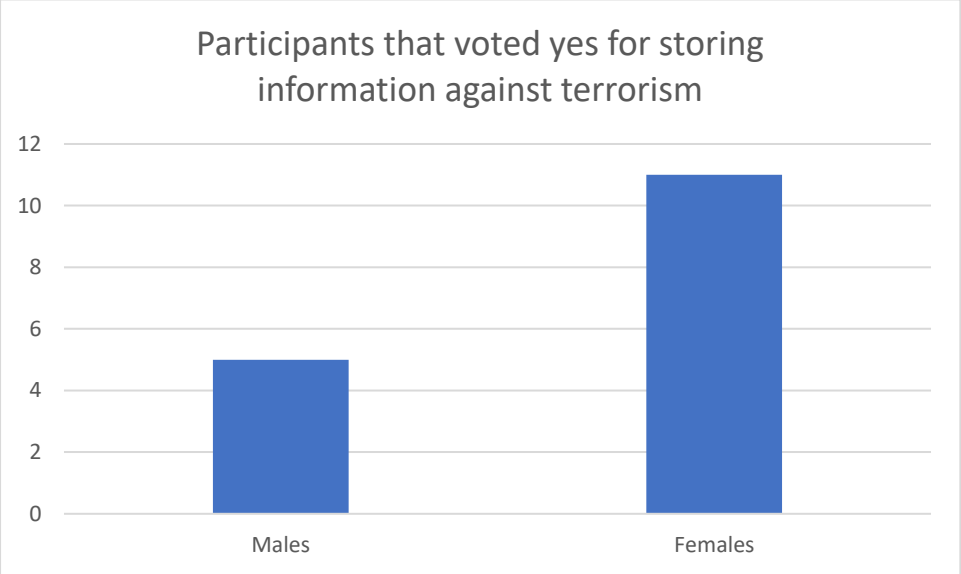
9) Should the Government share individual's data with other countries?

Results

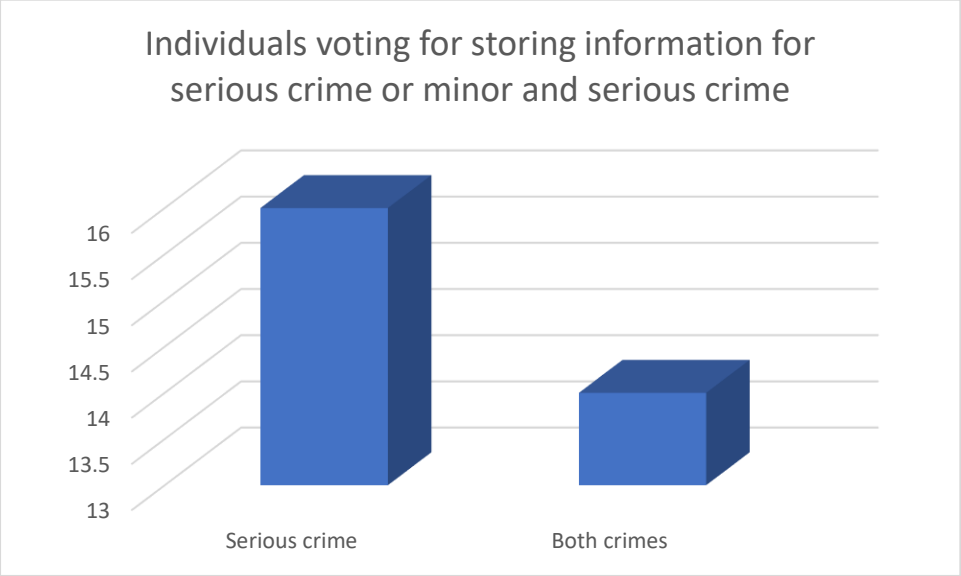
Participants were completely split on whether the Government store an individual's information, with a majority of males wanting independence from the authorities, while a majority of females were more open to the idea of the agencies storing information.



Here it is clear that females were open to agencies having access to data. When also using age as a comparison, younger people prefer to have more privacy rather than the older age groups. This shows that the younger generation, the individuals growing up with the newer methods of technology, would prefer for the Government to have less information on them.

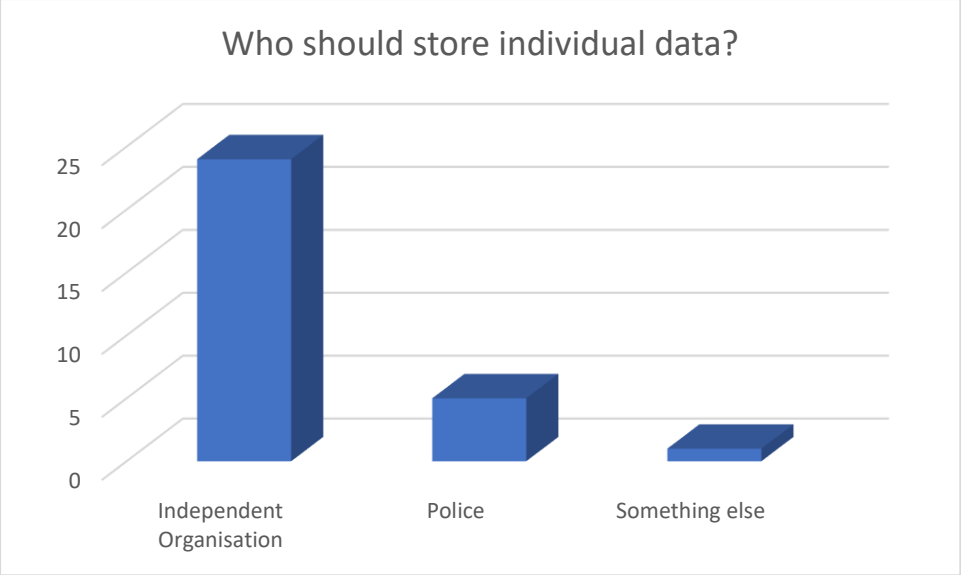


Most individuals answered that if they had to, they would allow the Government access to their data for the purposes of serious crime.



Here it is clear, that individuals prefer the legislation that explains that powers are used for serious crime and terrorism, making the Government compliant with the standards individuals have set out. When reviewing the minority, they all reported that they would feel more comfortable having both serious and minor crimes to be monitored. It could be argued that there is some crimes which are in the middle between both spectrums, and individuals feel that they need to be reviewed too.

A large majority wanted an independent organisation to ensure powers were correctly used and data stored, while a minority said the police.



The evidence here is clear that individuals may feel that the Government has currently too much power, and the need to have an independent organisation allows responsibility of holding information, while ensuring that a company would have to be held accountable to the Government. Currently, the agencies are self-accountable meaning that individuals may question how powers are used correctly. It shows that in the past, the Government has misused and abused legislation as they do not have an organisation to account to. The concern shows the need for this dissertation, to question whether the Government will use legislation and powers to ensure privacy and intrusion rights are used proportionally and not against the law.

Future studies

if in the future a study was to be conducted based on the evidence shown above, it would be interesting to find out the ethnicity of individuals and how they feel about the same subject, as white, black or Asian orientation may have different perspectives on privacy, intrusion by the Government and its agencies and methods used to store data.

At this point there would be new privacy/intrusion laws that may be the newest scandal, so whoever may be conducting the study may want to give a brief underpinning of new legislation to participants, and then give them a similar questionnaire based off of their thoughts of the new law.

By using focus groups, interviews or even more open ended questions allow participants to be more analytical about their answers, which may result in a better study. The purpose of questionnaires was to gain statistics within this dissertation, while a focus in the future could be on how media officials, journalists or whistle-blowers view certain laws. Already Edward Snowden has given his interpretation towards the Investigatory Powers Act, meaning more high ranking individuals who give a qualitative answer may make the study more substantial.

As a final example, by breaking the age groups down further to give a better understanding of whether it is a specific set of ages that oppose/prefer the legislation to allow data storage and usage. Within the questionnaire set out within this study, three age brackets were used to show a difference in thought.

<u>Conclusion</u>

To conclude the findings within the study clearly answer some research objectives, while also giving an understanding into the research question:

- Is there a need to reform the current system in place to allow an independent organisation to have control over powers?

Here, it is clear that individuals feel that powers the Government have should belong with an organisation. This does not mean to say individuals feel that the Government is doing

a bad job, rather that the most preferred choice is with an Independent organisation that the Government will be more duty bound to uphold to the law on data storage and usage. Currently the Government is self-analysing its own performance, and the question gives rise as to whether it should. The problem here is that if the Government could make a wrong decision the public may not find out until an enquiry is made. Whereas if an independent organisation was to make the same decision, this would either be leaked or found out, making the Government imposes fines and possible imprisonment for potential breaches of law.

It would be interesting to find out, a few years after the Investigatory Powers Act as to whether individuals prefer an independent organisation more, or whether agencies and the Government should still hold the powers to store and use personal sensitive information. Following Snowden's comments regarding the laws extensive privacy breaches, it appears that by allowing the Government to have this much authority allows for the dystopian state to become increasingly more surveillance based against the public in an Orwell type system.

- Should minor crimes be monitored?

Currently the law dictates that only serious crime and terrorism is to be focused on by the Government and its agencies. Within this study participants feel the same in regards to this, in the sense that a majority of individuals were happy to allow data storage for purposes of terrorism, while another majority believed serious crime was something to be monitored. It should be worth noting here that a proportion of individuals also felt that minor crimes should be monitored too, which in the future the Government may need to review. The

concern here is the Orwell type system is getting dangerously closer to being reality rather than fantasy.

Two of three research objectives here have been met, and should in the future be reviewed to compare whether the public adopt the same approach to the idea of data storage and use. When finally reviewing the research question, whether individuals felt that the Government have too much power, it could be considered within the question regarding an independent organisation that participants have already answered this. If they felt that the Government had a fair and proportionate amount of power, while they act based on necessity rather than storing mass amounts of data for an amount of time, then there would be no need for an independent organisation to take control. The idea of giving an independent organisation the powers is to ensure that agencies and authorities do not hold all control over individuals, when currently they do. Here it could be arguable to consider whether the research question has been met to assess if privacy and intrusion has met a balance, but to say that the Government has too much power could show that currently the rights of individual privacy rights are not being proportionately used.

6 - Conclusion and Recommendations

The purpose of this dissertation was to assess the Investigatory Powers Act and previous legislation surrounding privacy and intrusion rights, to assess the balance between the two aspects through the use of literature reviews, legislation and throughout questionnaires.

The Investigatory Powers Act has been created to "investigate, prevent and supress terrorism" due to the rise of terrorist threats. The United Kingdom has responded by implementing legislation, to attempt to try to deter crime and terrorism. This was done with the first pieces of legislation, the Regulation of the Investigatory Powers Act to the Investigatory Powers Act. The implications were privacy and intrusion based, specifically with communications data on technology. The powers set out within the new Act have allowed the Government to investigate data of individuals.

Although this is intrusive, it is justifiable and warranted to prevent terrorism, whereas it is unwarranted to allow individuals to be branded as criminals. The Act, and previous legislation is leading members of society to assume that they are potential criminals, because they are being treated the exact same. The requirement to assess is there is a need for legislation review is clear, as even now Members of Parliament are going through the Court system to give more privacy rights for individuals. Previous legislation has suggested that Human Rights is being abused, and that the UK Government is going beyond their powers.

The idea that the Government is becoming a dystopian surveillance state, suggested by Orwell does show that there was a need to assess legislation to make a proportional balanced argument for both acquiring individual information, while also ensuring privacy rights are maintained. Although the need for privacy rights is necessary, all legislation reviewed relates to how rights are intruded upon, and how the Government is trying to

justify their abuse of powers by using terrorism on a wide scale to ensure data is collected. Although newer forms of terrorism have been created (IE cyber terrorism), the Government are still accessing individuals information in non-terrorism related cases. This creates the argument of why individual's details are being monitored and recorded when they are unrelated to terrorism, or have not committed a crime.

Another aspect that needed to be considered is whether minor crimes should cause individuals information to be used. It appears that individuals are more willing to have their information used more for major crimes or terrorism than minor crime. This is due to the necessity aspect of what individuals are viewing for themselves. By using the powers within legislation to find minor crimes is unnecessary and unwarranted.

Privacy and intrusion concerns remain one of the biggest concerns for some individual's private lives, as whistle-blowers believe that the "the most extreme surveillance" has been introduced, and to monitor and review this further is needed to consider if abuses of privacy will occur more in the future. Currently, the Investigatory Powers Act is following previous legislation, and will use the powers given unnecessarily to force the privacy rights of individuals to be intruded on to try to counter terrorism.

The Government have been able to self-assess its own agencies, and there clearly is a need for an independent organization to review when powers are used and abused. The use of a company performing this would enable the Government to ensure that they are correctly using the powers, while also allowing an external examiner to assess when powers are abused. The concern currently is that the Government is abusing powers, assessing them and when the media eventually finds out, sparks outrage and injustice due to potential bias. This would lead to completely impartial verdicts, rather than a self-analysis which causes fear of injustice.

The Investigatory Powers Act has made it compulsory for Internet Service Providers to store individual's information. The Government and its agencies can view information, and assess whether there is a potential or current threat to society and national security in the information they review. This creates the stigma of an individual being a potential criminal, and sparks concern of using technology as the Government are building a profile of society and branding them potential threats. The power the agencies currently have is too much, allowing personal sensitive data to be used by external threats, leading society to believe that an 'Orwellian' style state is needed and that all individuals should be spied on.

Research objectives

The objectives within this dissertation were to establish where previous laws failed, and show if the Investigatory Powers Act would have its powers abused. This was done by reviewing previous misuses of power, led by the collection and intrusion of individual's personal sensitive information. This should establish whether privacy and intrusion are balanced, and if there is a need for a reform of the current system put in place. Although the Government can take and store information, privacy is breached, and has been in previous legislation, as the Governments have overused powers to monitor minor crimes, rather than deter terrorism and serious crimes. Legislation has been incorrectly used in the past, shown by the many cases being presented through the Court system involving Human Rights. The Government is continuing to collect information on a large scale, which allows the identification of individuals and their information to be invaded. The concern is that the Government has become a dystopian surveillance state, which allows society to be monitored, labelled as criminals, and waits for an individual to create an act (regardless of how small) and brand them as a criminal. Orwell's demonstration of this clearly shows that the Governments approach needs reforming before it becomes obsessed with the idea of

micromanaging individuals lives, to the point where they can spot an anomaly and assume a crime will occur (which is essentially being done).

When reviewing privacy, it is clear the Human Rights Act appear to be ignored by the Government, to allow data to be collected. The abuse of privacy in the past has been clear, and the justification around the modern day (shown through the legislation and literature reviews) suggests that privacy may become obsolete as Governments try to counter terrorism and crime. The Investigatory Powers Act is only the newest piece of legislation that allows this, showing that the privacy lives of individuals have and will continue to be affected, and that the Government is more concerned on collecting data and using the information for its own purposes.

Therefore, the Government should not have access to the amount of information currently accessed and monitored. The personal sensitive data is intended only for one person, and whom they wish to share this with, rather than having their rights violated to target criminal actions, especially minor crimes that are not warranted. By using all of societies information shows an unbalanced framework, rather than targeting associates of serious crime and terrorism.

This dissertation has questioned the role of privacy in society, in a domain that is heavily monitored. The argument that individual privacy rights are being intruded upon to attempt to protect the interests of the nation is a reasonable request, if this is purely for the purposes of serious crime and terrorism. This has been assessed under a proportionate and necessity based situation for some students, as all members of society are not going to comment a serious crime or terrorism. However, there are extremists that will, and the need to monitor all individuals to deter this is key. It does not mean that minor crime should

be monitored as this is something that is deemed to not be in proportion or even in the realm of necessity to have societies data recorded and used.

The idea to some scholars is that privacy is becoming an obsolete feature in a rapidly advancing technological age, and the only way to keep individuals safe is to monitor behaviour and counter any form of crime. To a degree, this is true as the idea to remove all terrorism in the world would be key. However, is then allows the Governments to become too powerful and allows further room for misuse of power.

When discussing intrusion, the Orwellian state is sprung to mind in several literature reviews, as a theme continuously mentioned throughout the reading of articles and journals. The fear Orwell presents is of a super state monitoring all individuals while invading their private lives. Privacy activists have begun to feel that their rights are being ignored, and it could be argued that the public could also think this in the future if further extreme legislation comes into force. Members of Parliament are beginning to question why the Government is allowing agencies to access powers within the Investigatory Powers Act, which allows the use of mass amounts of data that has been recorded. The concern here is that the Government has overstepped its obligations to ensure the nation is secure, to the point that it begins to question and analyse its own citizens. This has previously occurred within the Belmarsh case, and it could be argued that this will happen again.

When using phones and the internet as an example, both are being increasingly used as the digital age is occurring. Information can be extracted and stored from multiple sources, regardless of how necessary it is. The Government is using the information to deter crime and terrorism, based on the information it collects, but brings into question when the Government should stop harvesting information. Privacy and intrusion are unbalanced, regardless of national security, and it will only be a matter of time until it is able to truly

establish how far the Government has overstepped its powers with the Investigatory Powers Act. Proportionality and necessity have therefore been overlooked in a society that is continuing to grow technologically, and the Government is doing little to ensure the privacy rights of individuals are maintained, while the intrusion of data is expanding.

Alternative Methodologies/ Recommendations

One further methodology that could be used in a future study is a comparative approach relating to another country's privacy laws. By reviewing the US, Asia or the EU's approach could show a contrast of opinions between Governments, which could also show a change for legislation. If another country believes in privacy for individuals – and has lower crime or terrorist rates, then perhaps the UK should consider adopting a similar model to deterring these approaches.

This will show the privacy rights citizens in another country have, and the possible violations of their rights, while considering how the citizens in the UK have a balance in comparison to those abroad. This approach could be the next step when assessing how privacy laws interact across borders with another country. Alternatively, the evidence found could indicate that the UK has better privacy rights for individuals, in comparison to other countries. An example would be that within the EU, data retention can be extended for up to 2 years. Although the UK is in the EU, they have opted for a reduced storage period, showing that other countries could be longer, and potentially violate more rights.

Another approach would be to consider focus groups or interviews with specialists and members of the public to establish an emotive or literature based approach towards the qualitative methods. This would be able to establish, and give a more in-depth analysis

rather than the statistical approach taken by the questionnaires used in the study. This would give further evidence of acceptance or rejection from the UK population.

It is necessary to conduct research in this field further, especially regarding the Investigatory Powers Act, as this is still new legislation. If this were to be conducted five years later, this would either prove or disprove the evidence in this dissertation to suggest that privacy rights are being abused, and that individuals' lives are being intruded upon for data, rather than terrorism and serious crime.

Another way of reviewing this in the future is to look at: tracking, CCTV, monitoring conversations with technology, watching individuals through cameras, and by tracking individual's offline. As privacy and intrusion is so vast, it could be argued that this topic may never reach a result where the balance is truly struck, and instead newer and different technology and methods are brought in to be discussed whether they should be private, or open to the Government.

Conclusion

To conclude, it would appear at this current stage that previous legislation has been abused and could possibly in the future, shown through legal cases and commentary being presented by scholars and specialists (whistle-blowers, media, and officials within the surveillance spectrum). This has been reviewed, and the Government has implemented new legislation which should alter how the balance between privacy and intrusion is created. This was done by the Investigatory Powers Act, which could be argued that this still not has been achieved. It would appear, that even at the early stages there is a need for review, reform and change in the legislation that the UK population is being subjected to. The extent of this is that privacy rights are being abused, and some would consider this to

become obsolete in the wake of an advancing technological age with newer ways to commit crimes and terrorism.

Agreeably, information should be used to counter and deter terrorism and serious crimes, but should not for the smaller minor crimes that clearly have been previously used, and it is possible could be used again. The abuse of power used for this needs to be met with commentary from an independent source, away from the Government's control to be able to establish a bias free and transparent decision on cases that need to be discussed. Currently, this is not happening, and it could be argued that this may not happen anytime soon as more pressing issues have entered the realm of politics (Brexit), which may alter the idea of privacy altogether (pending the Governments decisions.

Therefore, it is necessary to review this again in the future, to consider whether the Government is going to abuse new legislation to force all crimes to be monitored, or whether there is a review of the current framework put in place to establish a balance, and more privacy rights for individuals. The purpose of privacy within a society is to be unidentified, and unfortunately in this instance currently in the UK this is not occurring, to the point where specialists, individuals, and whistle-blowers are considering returning to previous methods to communicate with individuals as it is less identifiable and traceable.

Word Count: 20,502

Bibliography

Books/Journals

A Acquisiti, 'What is Privacy Worth?' [2013] The Journal of Legal Studies (42)2
Alan Travis, 'Government wants phone and internet providers to track users' The Guardian [2009] https://www.theguardian.com/uk/2009/apr/27/home-office-superdatabase-email-phones accessed 03/06/17
Andrew Griffin, 'NHS Cyber Attack: North Kora Is Behind Hack That Bought Chaos To Hospitals, Experts Claim' Independent (2017) http://www.independent.co.uk/news/uk/home-news/nhs-cyber-attack-hack-north-korea-who-behind-hospitals-hackers-lazarus-a7738026.html accessed 19 May 2017

A Quelhas et al, 'Biases in questionnaire construction: how much do they influence the answers given?' [2011] Faculdade de medicina uniersidade do porto
Article 29 Data Protection Working Party, 'Opinion 3/2010 on the principle of accountability' [2010] 00062/10/EN WP 173
Astrup, 'RIPA Powers only used by Poole council twice since 2009 after spying outrage' [2016] http://www.bournemouthecho.co.uk/news/14183694.RIPA_powers_only_used_by_Poole_council_twice_since_2009_after_spying_outage/ Accessed 12 June
Big Brother Watch, "A Legacy of suspicion: How RIPA has been used by local authorities and public bodies" [2012]
Big Brother Watch, 'The Grim RIPA' [2010] Cataloguing the ways in which local authorities have abused their cover surveillance powers
Burgess, 'What is the IP Act and how will it affect you?' http://www.wired.co.uk/article/ip-bill-law-details-passed Accessed 12 June 2017
Castro & Mcquinn, 'The Privacy Panic Cycle: A Guide to Pulic Fears About New Technologies' [2015] Information Technology & Innovation Foundation
C Brown, 'Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice' [2015] International Journal of Cyber Criminology 9(1)
Christian Leuprecht, 'Government Information Quarterly' [2016] 33(2) Beyond the Castle Model of cyber-risk and cyber-security pg 2502-57; Denis Campbell, Haroon Siddique, 'Operations Cancelled As Hunt Accused Of Ignoring Cyber-Attack Warnings' The Guardian (2017) https://www.theguardian.com/technology/2017/may/15/warning-of-nhs-cyber-attack-was-not-acted-on-cybersecurity accessed 19 May 2017
Chris Holder, 'Computer Law & Security Review' [2016] 32(4) Robotics and law: Key legal and regulatory implications of the robotics age (Part II of II) pg 557-576; Robert Booth, 'Cyber-Attack Set To Escalate As Working Week Begins, Experts Warn' The Guardian (2017) https://www.theguardian.com/technology/2017/may/14/cyber-attack-escalate-working-week-begins-experts-nhs-europol-warn accessed 18 May 2017
Chris Johnston, 'TalkTalk customer data at risk after cyber-attack on company website' The Guardian [2015] https://www.theguardian.com/business/2015/oct/22/talktalk-customer-data-hackers-website-credit-card-details-attack accessed 03/06/17
Claire Macken, Counter-terrorism and the detention of suspected terrorists (1st edn, Routledge 2013)
C Nyst, 'The right to privacy in the digital age' [2017] Journal of Human Rights Practice, 9(1) 104-118
Claire Walker, 'Computer Law & Security Review' [2009] 25(4) Data retention in the UK: Pragmatic and proportionate, or a step too far? Pg 325-334
C Walker, 'Data Retention in the UK: Pragmatic and Proportionate, or a step too far?' [2009] Computer Law & Security Review (25)
'Computer Fraud & Security' [2017] 2017(1) Snoopers' Charter under attack pg 3; The Guardian, 'The Guardian View on the Draft Investigatory Powers Bill: Snooper's Charter 3.0' The Guardian (2015) https://www.theguardian.com/commentisfree/2015/nov/02/the-guardian-view-on-the-draft-investigatory-powers-bill-snoopers-charter-30 accessed 19 May 2017
Custers et al, 'Fear effects by the media' [2012] 171(4) European Journal of Pediatrics
C Williams, 'Research Methods' [2007] Journal of Business & Economic Research (5)3
Danny Boyle, Melanie Hall, 'Borussia Dortmund Explosions: Islamist Suspect Arrested Over Bus Bombs As Prosecutors Investigate 'Terrorist Link' The Telegraph (2017) http://www.telegraph.co.uk/news/2017/04/12/borussia-dortmund-bus-bombing-police-probe-islamist-letter-referring/ accessed 19 May 2017
David Anderson, 'Surveillance Powers: New Law Needed, Says Terror Watchdog' BBC News (2015) http://www.bbc.co.uk/news/uk-33092894 accessed 19 May 2017; David Anderson, 'A Question of Trust
D Brennan, 'Still a 'Safe' Harbor? – implications of Schrems v DPC' (7)5 Data Protection Ireland
D Collier, 'Qualitative versus Quantitative: What might this distinction mean?' [2003]
Don't Spy On Us, 'Snoopers' Charter Could Hit Police Forces with £1 Billion Bill' [2016] Proposals to collect the internet connection records (IRCs) of every UK Citizen could cost more than £1 billion. There costs, which would fall to the Home Office, could be the equivalent cost of employing 3,000 full-time police officers at a time of office cuts. https://www.dontspyonus.org.uk/blog/2016/03/30/%E2%80%98snoopers%E2%80%99-charter%E2%80%99-could-hit-police-forces-with-%C2%A31-billion-bill/ accessed 03/06/17
D Lyon, 'Technology vs terrorism: circuits of city surveillance since September 11th' [2003] International Journal of Urban and Regional Research (27)3

Echevarria, Morales et al, 'An E-government Interoperability Platform Supporting Personal Data Protection Regulations [2016] 19(2) CLEI Electronic Journal
Edward Snowden, '@Snowden' (Edward Snowden's Twitter Account, 17 November 2016) https://twitter.com/snowden/status/799371508808302596?lang=en accessed 19 May 2017
European Council, 'Declaration on Combating Terrorism' [2014]
George Orwell, 'Nineteen Eighty-Four' (1st edn, Secker & Warburg 1949)
G Robert, 'Critical legal histories' [1984] Stanford Law Review 57
Harriet Harman, Joint Committee on Human Rights Chair; Legislative Scrutiny: Investigatory Powers Bill First Report of Session [2016-2017]
Helen Fenwick, 'International Review of Law, Computers & Technology [2011] 25(3) Counter-terror strategies, human rights and the roles of technology pg 107-115; Matt Dunham, 'London Attack: The Terrorist, The Bloody Aftermath And His Victims' The Telegraph (2017) http://www.telegraph.co.uk/news/2017/03/22/westminster-attack-pics/ accessed 19 May 2017
HM Government, 'CONTEST: The United Kingdom's Strategy for Countering Terrorism' [2011]
Home Office, Government response to 'Repeal the new Surveillance laws (Investigatory Powers Act) (3rd May 2017) https://petition.parliament.uk/petitions/173199 accessed 19 May 2017
Home Office, 'Investigatory Powers Bill European Convention On Human Rights Memorandum' (2015) https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473763/European_Convention_on_Human_Rights_Memorandum.pdf accessed 19 May 2017
James Murray, Oxford Dictionary of English (Oxford University Press 2010)
James Titcomb, 'Petition to repeal new surveillance powers reaches 100,000 signatures' The Telegraph (2016) http://www.telegraph.co.uk/technology/2016/11/28/petition-repeal-uks-new-surveillance-powers-reaches-100000-signatures/ accessed 19 May 2017
Jenny Jones MP, Green Party, https://www.youtube.com/watch?v=3I3olv3u-fI&feature=youtu.be
Joe Stevens, 'Journal of Terrorism Research' [2012] 3(2) Implementing 'targeted' UN Sanctions in the UK: Is Freezing of Terrorist Assets Giving Fundamental Rights the Cold Shoulder?' pg 1-10
J Roberts et al, 'The Invisible addiction: Cell-Phone activities and addiction among male and female college students' [2014], Journal of Behavioural Addictions
J Petley, 'Panic Stations: Surveillance in the UK' [2013] 42(1) From online activity to terrorism laws, the government continues to make decisions based on fear and ignorance argues Julian Petley
J Sale, 'Revisiting the quantitative-qualitative debate: Implications for mixed-methods research' [2002]
Julian Petley, 'Panic Stations: Surveillance in the UK' [2013] 42(1) pg 70
J Wesley, 'American Educational History Journal' [2011] (38)1,2
K Meadows, 'So you want to do research? 5: Questionnaire design' [2003] British Journal of Community Nursing (8)12
K Rawlinson, 'Snoopers' Charter? That's's the least of your worries' [2012] The Independent, http://www.independent.co.uk/life-style/gadgets-and-tech/news/snoopers-charter-thats-the-least-of-your-worries-7854798.html Accessed 12 June
Madhumita Murgia, George Parker, Jim Brunsden, 'EU's highest court declares UK surveillance powers illegal' Financial Times (2016) https://www.ft.com/content/f847f522-c761-11e6-8f29-9445cac8966f accessed 19 May 2017
M Salter, 'Writing Law Dissertations: An introduction and guide to the conduct of legal research' [2007]
National Crime Agency, 'National Cyber Security Centre' [2016/2017] The cyber threat to UK business
N MacCormick, 'Four Quadrants of Jurisprudence' [1994] Percriptive Formality and Normative Rationality: Essays in Honour of R S Summers 53-70
'Network Security' [2016] 2016(2) Impending Investigatory Powers Bill comes under fire pg 1-2; The Guardian, 'The Guardian View on the Draft Investigatory Powers Bill: Snooper's Charter 3.0' The Guardian (2015) https://www.theguardian.com/commentisfree/2015/nov/02/the-guardian-view-on-the-draft-investigatory-powers-bill-snoopers-charter-30 accessed 19 May 2017
Open Rights Group, 'Communications Capabilities Development Programme' [2012], The Communications Capabilities Development Programme has now, as of May 2012 produced proposed legislation, the draft Communications Data Bill.
Privacy International, 'Mass Surveillance' https://www.privacyinternational.org/node/52
P Wragg, 'Privacy and the emergent intrusion doctrine' [2015] Journal of Media Law (9)1
Privy Counsellor Review Committee, 'Anti-terrorism, Crime and Security Act 2001 Review: Report' [2003]

Report of the Investigatory Powers Review' June 2015, https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Web-Accessible1.pdf accessed 19 May 2017
R Jones, 'UK data retention regulations' [2008], Computer Law & Security Report (2)4
R Little, 'Journal of survey statistics and methodology' [2017] Oxford University Press (5)4
Robert Mendick, 'Russian-Linked Cyber Gang Blamed For NHS Computer Hack Using Bug Stolen From US Spy Agency' The Telegraph (2017) http://www.telegraph.co.uk/news/2017/05/12/russian-linked-cyber-gang-shadow-brokers-blamed-nhs-computer/ accessed 19 May 2017
Rt Hon Sir Paulk Kennedy, 'Report of the Interception of Communications Commissioner for 2009' [2009]
Siad Shanin, 'Journalism & Mass Communication Quarterly' [2016] 93(2) Right to Be Forgotten: How National Identity, Political Orientation, and Capitalist Ideology Structured a Trans-Atlantic Debate on Information Access and Control pg 260-382
Steve Saxby, 'Computer Law & Security Review' [2013] 29(1) The 2012 CLSR-LSPI seminar on privacy, data protection & cyber-security - Presented at the 7th international conference on Legal, Security and Privacy Issues in IT law (LSPI) October 2-4, 2012, Athens 4-12
Suhang et al, 'Impact of Excessive Mobile Phone Usage on Human' [2016], Human. J Computer Science System Biology
'The New Criterion' [2016] 34(5) Who speaks for Islam? Ph 1-4;Jason Burke, 'ISIS Celebration Over The London Attack Is A Dance of Defeat' The Guardian (2017) https://www.theguardian.com/uk-news/2017/mar/24/isis-celebration-over-the-london-attack-is-a-dance-of-defeat accessed 19 May 2017
The Report of the IOCCO Inquiry into the Use of Chapter 2 of Part 1 of the Regulation of Investigatory Powers Act (RIPA) to Identify Journalistic Sources [2015]; P Bernal, 'Data gathering, surveillance and human rights@ recasting the debate' [2016] Journal of Cyber Policy (1) 2
T Weir, 'The Limits of Liability: Keeping the Floodgates Shut' [1999] 58(3) The Hague, London, Boston: Kluwer Law International
Warren, Brandeis, 'Harvard Law Review' [1890] 4(5) The Right To Privacy
W Williams, 'A Sampler on sampling' [1978], Wiley (141)2

Cases

A and Others v. Secretary of State for the Home Department 2004 UKHL 56
C-131/12 Google Spain SL, Googlge Inc v Agencia Española de Protección [2014] ECJ
HM Treasury v Ahmed 2010] UKSC 2
J Barlett, Orwell v Terrorists [2015]
R v Secretary of State for the Home Department ex p David Davis MP, Tom Watson MP, Peter Brice and Geoffrey Lewis [2015] EWCA Civ 1185
Schrems v Data Protection Commissioner [2015] Case C-362/14

Legislation

Anti-Terrorism, Crime, and Security Act 2001
Counter Terrorism Act 2008
Counter-Terrorism (Temporary Provisions) Bill 2008
Data Protection Act 1998
Data Retention (EC Directive) Regulations 2009
Draft Data Communications Bill 2012
Human Rights Act 1998
Investigatory Powers Act 2016
Prevention of Terrorism Act 2005
Regulation of the Investigatory Powers Act 2000
Statutory instrument 2007 No. 2199
Terrorism (United Nations Measures) Order 2006
Terrorism (United Nations Measures) Order 2009