Access to Electronic Information: How the Requirements of Modern Day Criminal Investigation and Prosecution Have Unduly Limited Citizens' Criminal Procedure Rights

By Findlay Glynn

LL.M in Human Rights Long Thesis

Supervisor: Dr. Petra Bárd

Central European University

1051 Budapest, Nador utca 9.

Hungary

Contents

Executive Summary

Chapter 1: The Forced Disclosure of Electronic Information

This chapter analyses the employment of key disclosure legislation, where suspects to a crime are compelled to decrypt electronic devices under threat of criminal sanction. The use of such provisions has been most prominently seen in the investigatory practices of the United Kingdom, who have taken great legislative steps to gain access to a significant amount of information from their citizens. This is compared with the position emanating from Germany, who due to a historically influenced dedication to the protection of encryption, have refrained from replicating the above key disclosure laws, and instead have attempted to access the same degree of information without the suspect's knowledge. These provisions are analysed under the privilege against self-incrimination, which on its face would be likely to be violated by the forced disclosure of a password. However due to the lack of coherence in its theoretical rationales and judicial interpretations, and the number of exceptions provided by bodies such as the European Court of Human Rights, the answer is not so clear. Therefore, the various different situations in which key disclosure provisions operate are subjected to a comparative analysis of the jurisprudence of the UK, Germany, the European Court of Human Rights (ECtHR), and several other international jurisdictions, to determine where and when this investigatory technique will violate the privilege against self-incrimination.

Chapter 2: Surveillance and its Impact on the Presumption of Innocence

The second chapter proceeds to evaluate investigatory surveillance which, due to the vast amount of information stored online and on electronic devices, has become an increasingly used by domestic authorities in their operations. Although the whistleblowing of Edward Snowden in 2013 led to surveillance practices becoming more transparent, the United Kingdom and Germany have continued to advance their covert monitoring, including

the deployment of pre-crime investigations, in which they attempt to prevent crimes before their commission. In all of the jurisdictions studied, civil liberties advocates have successfully argued that the use of this surveillance violates the right to privacy, which has greatly limited such Government action. However, this chapter instead analyses state monitoring under criminal procedure rights, concluding on whether arguments could additionally be made under the presumption of innocence. Whilst the judicially recognised interpretation of this right would only act to restrict the use of surveillance when the suspect is then charged, arguing under theoretical expansions of the presumption encompassing the "right to be trusted" and the "right not to be stigmatised as criminally suspicious" could also limit the use of mass surveillance on all citizens, in both the pre and post crime contexts.

Chapter 3: Evidentiary Rules and Electronic Evidence

The final chapter considers the effect that the previous arguments based on criminal procedure rights will have on the use of the electronic evidence obtained at trial. Ordinarily, the exclusion of evidence in the domestic jurisdictions of the United Kingdom and Germany has been left to the discretion of the trial judge, where the legality and human rights compliance of how it is obtained is often inconsequential. With regard to electronic evidence obtained under key disclosure and surveillance, despite some legislative exclusions, the decision on admissibility is often determined through a proportionality analysis, taking into account the gravity of the interference with fundamental rights, and the seriousness of the offence charged. In the jurisprudence of the three jurisdictions covered, it is clear that arguments under the right to privacy, often used to challenge the above practices, will not lead to the exclusion of the collected information. On the other hand, where the evidence has been shown to be obtained in violation of a criminal procedure right, such as the privilege against self-incrimination, or the presumption of innocence, the judge will have no choice but to rule it inadmissible.

Introduction

"Sniff it all – Know it all – Collect it all – Process it all – Exploit it all".[1] The primary aims of criminal investigation have remained a constant throughout time, as domestic authorities have sought to detect, prevent, and prosecute unlawful actions. Traditionally, this would be achieved through the use of covert operatives, intelligence gathering, and crime scene investigation, where physical evidence and confessions would be used to arrest and punish offenders. In later years, the establishment of video, audio, and postal surveillance permitted the investigating authorities to conduct their operations from a distance, whilst maintaining their ability to monitor suspects in their planning and commission of misconduct.

However, following the advance of the internet and mobile communications, the majority of the preparation for criminal activities has become facilitated by electronic devices, making it increasingly difficult for investigators to gather evidence. What was previously discussed in darkened rooms or alleyways is now communicated over instant messaging applications and stored online, leaving no physical trace, and thus evading the previous investigative techniques used. Furthermore, as this information is often destroyed or encrypted following the offence, it has become near impossible for the police to obtain evidence in the subsequent investigation. Therefore, domestic authorities have had to adapt the way they approach their operations, moving to address these 21st Century issues by harnessing the technology available, and thus ensuring that the effectiveness of their operations remains constant.

Nevertheless, these developments have also provided the state with the potential to move far beyond their previous capabilities, to the point where they can now access an

[1] Taken from a NSA document titled 'New Collection Posture', G Greenwald, No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State, Toronto: McClelland & Stewart, 2014. R Whitaker, *The Politics of the Right*, New York, 2015, pg. 347

unprecedented amount of information about their citizens. The almost universal use of internet connected devices means there is the potential for investigators to access information on where an individual has been, what they have been doing, and who they have been communicating with, at the click of a button. As noted by the US Supreme Court's Justice Brandeis, "[d]iscovery and invention have made it possible for the Government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet".[2] Therefore, various states have enacted laws granting direct access to such information, through either the interception of, or later intrusion on, the suspect's personal electronic communications and documents.

Due to the particularly intrusive nature of this action, it is clear that it has the potential to interfere with various fundamental rights. The majority of the scholarship and legal challenges on this topic thus far have centred on the impact that these practices have had on the right to privacy, under both domestic and international law. This is an entirely logical argument to make, and as will be later outlined, it has been relatively successful in reducing the power of investigating authorities around the world in their access of personal data. However, this proposition also has its limits, and by solely focussing on this singular right, civil liberties advocates and scholars have consequently failed to utilise all the mechanisms available to them. Authorities have gradually become wise to the restrictions that these arguments pose, and thus have adapted their legislation so as to comply with the right to privacy, while at the same time retaining the ability to collect vast amounts of electronic information from their citizens. Furthermore, domestic and international judiciaries, despite vastly expanding the scope of what the right to privacy will encompass, have also limited its

[2] *Olmstead v. United States*, 277 U.S. 473 (1928)

standing in the hierarchy of rights protection, resulting in the finding of a violation not having the full effect desired.

Therefore, this thesis shall instead evaluate the impact of such practices on criminal procedure rights, in particular the privilege against self-incrimination and the presumption of innocence. It will be shown that whilst the right to privacy will likely remain the first port of call when addressing these issues, criminal procedure rights offer an innovative, and potentially stronger protection against state interference with electronic information.

Firstly, this analysis will cover the practice of key disclosure, under which investigating authorities can compel suspects to decrypt their electronic devices, through threat of criminal sanction. A prima facie glance at this practice would indicate that it would constitute a clear violation of the right against self-incrimination, as it forces the accused to waive their right to silence, and possibly contribute to the case against them. However as will be illustrated, this is an issue yet to be tested before an international human rights judiciary, and national courts have not taken such a clear approach in respect of their own fundamental rights provisions. Thus, it becomes prudent to analyse the specific situations in which this conflict will occur, and through considering the tests set out in both domestic and international law for the privilege, conclude on if and when a violation will be likely to be found.

The use of surveillance on electronic devices could also lead to several issues with other due process rights, most notably the right to be presumed innocent. As various states move towards a ‘prevention’ orientated criminal justice system, the employment of untargeted mass surveillance has increased, which some theorists have argued creates stigmatization and an appearance of untrustworthiness in respect to innocent civilians. Furthermore, if the evidence obtained is used in trial, it may act to reverse the burden of proof

onto the applicant, as from the outset they will be at task to prove themselves innocent. Whilst the use of surveillance is yet to be recognised as undermining the presumption of innocence before a judicial body, the expansion of this right by the ECtHR indicates that there may be the possibility for such a finding. With this in mind, it will be established whether this theoretical position can be claimed to be a viable judicial alternative to arguments under the right to privacy, or if it will remain a contention resigned to abstract considerations.

Finally, this thesis will analyse whether electronic evidence obtained through the above practices should be deemed admissible at trial. Permitting the use of this information raises the possibility of various violations with fair trial guarantees, due to its arbitrary collection, and possible unreliability. Despite some states enacting statutory provisions to exclude this evidence, rules on admissibility are often left to be decided on a case by case basis. Once again, there is a discrepancy between the use of the right to privacy and criminal procedure protections in this respect, as evidence is far more likely to be struck out if shown to be in violation of the latter. Therefore, it is necessary to conclude whether this potential benefit justifies the efforts made to prove the access to electronic information as being contrary to criminal procedure rights, or whether civil liberties advocates should instead place their energy into strengthening and advancing arguments based solely on the right to privacy.

The above considerations will be analysed through a comparative analysis of the legal provisions and case law of the United Kingdom, Germany, and the European Court of Human Rights. In recent years, the United Kingdom has been the centre of controversy surrounding Government surveillance, where despite new legislation proclaiming to limit state power, UK citizens remain among the most at risk for having their communications and personal information collected by the authorities.

On the other hand, as a result of historical abuses of citizen's privacy during the operations of the Nazi regime and the Stasi, Germany has held a longstanding mistrust for state monitoring, leading to significantly strong constitutional protections restricting such actions. Nevertheless, in recent years this apparent 'German exceptionalism' regarding the privacy of citizens has begun to slip, as the Bundestag have granted German investigators significantly expansive powers in accessing electronic information. Furthermore, due to their civil law based judicial system and constitutional based liberties, Germany also provides an interesting comparator to the common law processes of the United Kingdom, especially when considering the potential success of innovative arguments based on criminal procedure rights.

The third and final jurisdiction of this analysis, the European Court of Human Rights, offers the greatest insight into whether criminal procedure rights can be said to be limited by state access to electronic information, and whether the arguments outlined will be likely to be successful. Although legislation and judicial decisions in the UK and Germany are greatly influenced by its jurisprudence, for the purposes of this analysis the ECtHR will be treated as a jurisdiction in itself, as it often provides a greater and occasionally differing level of protection to fundamental rights, especially in regards to the creative and speculative arguments outlined below.

Chapter 1: The Forced Disclosure of Electronic Information

i) Introduction

As noted above, due to 21st Century advancements in technology, the majority of the preparation and planning of criminal offences now occurs on electronic devices, making it increasingly difficult for investigating authorities to gather evidence. To combat this issue, various states have created laws authorising the direct access to such information. A common trend in expanding such investigatory powers has been the enactment of legislation requiring the disclosure of passwords from suspects. Following the arrest of an individual, these jurisdictions now permit policing authorities to compel a suspect to decrypt their devices under the threat of criminal sanction. A prima facie glance at this practice would appear to indicate a clear violation of the right against self-incrimination, as it not only forces the accused to waive their right to silence, but is also an equivalent to the handing over of the documents or hardware itself.

Furthermore, as a result of these technological developments, the wealth of information now stored on modern mobile devices makes these orders all the more threatening to fair trial rights. As noted by the US Supreme Court in a recent decision, modern smartphones "are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy".[3] A mobile phone is no longer simply used as a communication device, and is now more akin to a safe, where users will place copious amounts of information that they wish to keep private.[4] Therefore, is of no coincidence that these devices have become a very attractive target for investigating authorities.[5] What remains to be determined is if modern

[3] *Riley v. California*, 134 S. Ct. 2489 (2015)
[4] E Lemus, *When Fingerprints Are Key: Reinstating Privacy to the Privilege against Self-Incrimination in light of Fingerprint Encryption in Smartphones*, 70 S.M.U. L Rev 533, 2017, pg. 543
[5] A M Gershowitz, *Password Protected? Can a Password Save Your Cell Phone from a Search Incident to Arrest?*, Iowa Law Review, Vol. 96:1125, 2011, pg. 1128

fair trial rights are flexible enough to adjust to these developments in encryption technology, and provide adequate protection for the affected suspects.

ii) The United Kingdom

In evaluating the use of key disclosure provisions, it becomes apparent that in practice there are two primary uses. Firstly, investigating authorities may force the disclosure of a password where they believe that the electronic device contains evidence related to the charge for which the accused was arrested.[6] Failure to give such a key would amount to obstruction of justice in the classical sense, and through this, further sanctions may apply. The second function arises where the individual is detained not in lieu of an established offence, but instead to determine whether they have committed or assisted in the commission of any crimes. Resistance to this request will constitute an offence in itself, without the accused having necessarily been part of a crime or national security threat.[7]

These two approaches are most prominently apparent in the legislation of the United Kingdom. Through Section 49 of the Regulation of Investigatory Powers Act 2000 (RIPA), UK authorities can compel an individual to reveal their password or encryption key, in situations where they are detained due to suspicion of an offence. Investigating police officers are granted the power to provide an individual with a notice requiring disclosure in situations where any information that they have lawfully obtained is encrypted, and thus, inaccessible.[8] There must be reasonable grounds to suspect that the individual is in possession of the key, and the disclosure must be necessary in either "the interests of national security", "for the purpose of preventing or detecting crime", or "in the interests of the economic well-being of the United Kingdom".[9] If these requirements are fulfilled, and the disclosure complies with

[6] For example, s49 Regulation of Investigatory Powers Act 2000
[7] s2(4) Schedule 7 Terrorism Act 2000
[8] s49(1)(a)-(e) Regulation of Investigatory Powers Act 2000
[9] Ibid., s49(2)-(3)

various other procedural safeguards, then the notice may be granted.[10] Failure to comply with this request will result in an offence under Section 53 of the Act, punishable with up to two years imprisonment, rising to five years if the case concerns national security or child indecency.[11] The first convictions under RIPA for the failure to disclose an encryption key came in 2009.[12] As noted in the annual report of the Chief Surveillance Commissioner, of the fifteen notices served, eleven were not complied with, resulting in seven charges under Section 53, and two convictions.[13] Despite both the number of Section 49 notices issued, and refusals thereof, increasing since 2009, the number of convictions under Section 53 have remained relatively low.[14] Nevertheless, this legislation remains powerful threat to the rights of suspects, as illustrated by the judicial objections it has faced.

The case of *R v. S and Another* posed the most fundamental challenge before the UK Courts to the key disclosure requirement of RIPA.[15] This case concerned an application for leave to appeal, on the basis that a Section 49 order violated the privilege against self-incrimination, found under Article 6 of the European Convention on Human Rights (ECHR).[16] Following the breach of a control order, the defendants H and S were subject to lawful searches, in which the authorities found various encrypted computer hard drives.[17] In addition to charges for breaching the control order, both defendants were served with notices under RIPA, detailing that a failure to disclose the correct encryption key would result in a

[10] Ibid., s49(2), see s49(4) for further safeguards.
[11] Ibid., s53(5)
[12] *First RIPA convictions over disclosure of encryption keys*, Computer Fraud & Security, Volume 2009, Issue 9, Elsevier Ltd, September 2009, pg. 3
[13] *Annual Report of the Chief Surveillance Commissioner to the Prime Minister and to Scottish Ministers for 2008-2009*, Office of Surveillance Commissioners, HC 704, SG/2009/94, pg. 12
[14] For example in 2014-2015 there were reportedly 37 notices served, of which only 9 were complied with, and only 3 resulted in convictions under Section 53. *Annual Report of the Chief Surveillance Commissioner to the Prime Minister and to the Scottish Ministers for 2014-2015*, Office of Surveillance Commissioners, HC 126, SG/2015/56
[15] *R v. S & Anor*, [2008] EWCA Crim 2177
[16] Ibid., at [9]
[17] Ibid., at [3]

further offence.[18] The applicants claimed that forcing them to reveal possibly incriminating information violated their Article 6 ECHR rights.[19] The Court dismissed the appeal on the basis that the encryption keys had an existence independent of the applicants' wills, thereby falling out with the protection of the Convention.[20] Furthermore, the Court found that due to the minimal nature of the interference, the police's actions were both proportionate and permissible.[21] This construction of the privilege against self-incrimination by the Court of Appeal constitutes both a unique and questionable interpretation of the jurisprudence of the Strasbourg Court, which will be discussed in greater detail later in this chapter.[22] However, it is clear in any sense that the UK courts regard the issue of key disclosure as unproblematic to fundamental rights, signalling that future legal challenges to Part III of RIPA will also fall by the wayside.

Whilst disclosure requirements arising from Section 49 notices predominantly occur in connection with another suspected offence, UK law further permits authorities to compel the release of a password without direct suspicion of another crime. Schedule 7 of the Terrorism Act 2000 bestows UK border police with the authority to question and search individuals at any airport, train station, or ferry terminal.[23] Under this Schedule, an "examining officer"[24] can stop, detain, and interrogate anyone they believe to be a terrorist, thereby falling under Section 40(1)(b) of the Act.[25] Anyone interviewed has a legal duty to provide the examining officer with any requested information or documents in his possession.[26] The scope of the information required to be disclosed, provided by the

[18] Ibid., at [6] – [8]
[19] Ibid., at [9]
[20] Ibid., at [20]
[21] Ibid., at [25]
[22] See page 31 below.
[23] s1 Schedule 7 Terrorism Act 2000
[24] Defined under s1(1) Schedule 7 Terrorism Act 2000 as either a "constable", an "immigration officer", or a designated "customs officer".
[25] s2(1) Schedule 7, s40(1)(b) Terrorism Act 2000
[26] Ibid., s5

Government's Code of Practice for examining officers, includes "electronic data stored on electronic devices, and passwords to those electronic devices".[27] Therefore, this appears to grant examining officers with an equivalent power to that found under Section 49 of RIPA.

However, Schedule 7 goes one-step further, permitting such disclosure notices even where the officer has no concrete grounds for suspecting that the individual is a terrorist, and thus, involved in criminal activity.[28] The detention and search of an individual in order to determine whether they may be suspected of being a terrorist raises clear legal issues, as noted by various commentators on this legislation. For example, the former Chief Executive of the Equality and Human Rights Commission, Mark Hammond, questioned whether there was racially biased selection under the Act, remarking, "stopping people based on stereotypes could lead to time and resources being misdirected and have a negative impact on relations with black and ethnic minority groups".[29] This opinion has a statistical basis, with figures showing that those of an Asian ethnicity were disproportionately likely to be questioned and detained under Schedule 7.[30] Nevertheless, as noted by David Anderson, the former Independent Reviewer of Terrorism Legislation, "these statistics do not constitute evidence that those powers were being used in a racially discriminatory manner".[31] This finding was backed by the decision of *R (K) v. Secretary of State for the Home Department.*[32] In that case, the applicant sought judicial review of Schedule 7 on the basis that it contravened Section 4 of the Human Rights Act 1998.[33] Due to apparent irregularities in the applicant's passport, he

[27] Paragraph 39, Examining Officers and Review Officers under Schedule 7 to the Terrorism Act 2000, Code of Practice, Home Office, March 2015 (last updated 17 March 2016)
[28] s2(4) Schedule 7 Terrorism Act 2000
[29] *Asian people 11 times more likely to be stopped at UK borders, analysis finds*, A Travis, The Guardian, 5th December 2013, Accessed via https://www.theguardian.com/law/2013/dec/05/asian-people-stopped-uk-borders-analysis on 15/11/17
[30] D Anderson Q.C., The Terrorism Acts in 2015, *Report of the Independent Reviewer on the Operation of the Terrorism Act 2000 and Part 1 of the Terrorism Act 2006*, December 2016, 7.17 – 7.19
[31] Ibid., 7.18
[32] *R (K) v. Secretary of State for the Home Department*, CO 10027/2011
[33] Ibid. S Wood, *The Terrorism Act 2000 Schedule 7 and its Implications for the Human Rights of Passengers Travelling through United Kingdom Airports*, Global Security Studies, Winter 2015, Volume 6, Issue 1, pg. 15,

was detained and questioned under Schedule 7, leading to a claim that the legislation was being applied in a discriminatory fashion.[34] This appeal for judicial review was soundly rejected, with Collins J stating that:

The ability to stop and examine would-be passengers at ports is an essential tool in the protection of the inhabitants of this country from terrorism…I do not doubt that the claimant feels that he has been wrongly and unfairly treated since it is clear that he did not in the result appear to be a terrorist. But the power is necessary in a democratic society and, quite apart from the delay in seeking to challenge it, the contrary is not arguable.[35]

It is perhaps an unfortunate but inevitable consequence of the requirements of Schedule 7 that those detained will be disproportionately a member of an ethnic minority. Indeed, in deciding whether an individual can be suspected of being a terrorist, police authorities may be swayed by the fact that over fifty percent of all those convicted with terrorist-related offences in the UK were "of Asian appearance".[36] Nevertheless, under the Code of Practice, an individual's ethnic background cannot be used under any circumstances as the sole reason for their examination, ruling out the legal possibility of such a discriminatory selection.[37]

Further criticism has centred on the apparent indiscriminate use of Schedule 7, with Liberty regarding it as a "breathtakingly broad and intrusive power".[38] As previously stated, examining officers can question individuals under the Act without concrete suspicion that

[34] Ibid.
[35] D Anderson Q.C., The Terrorism Acts in 2011, *Report of the Independent Reviewer on the Operation of the Terrorism Act 2000 and Part 1 of the Terrorism Act 2006*, June 2012, 9.37. *R (K) v. Secretary of State for the Home Department*, CO 10027/2011.
[36] D Anderson Q.C., The Terrorism Acts in 2015, December 2016, 7.20
[37] Paragraph 19, Examining Officers and Review Officers under Schedule 7 to the Terrorism Act 2000, Code of Practice, Home Office, March 2015 (last updated 17 March 2016). *Beghal v. The United Kingdom,* Application no. 4755/16, Communicated Case, 2016.
[38] *Schedule 7*, Liberty, Accessed via https://www.liberty-human-rights.org.uk/human-rights/countering-terrorism/schedule-7 on 15/11/17

they are a terrorist.[39] However, this power is severely limited by the accompanying Code of Practice, where authorities are instructed that their selection must not be arbitrary, and must strictly be related to, and informed by, a threat of terrorism to the United Kingdom.[40] They are under a duty to "take into account considerations that relate to the threat of terrorism", defined by the Code of Practice as factors ranging from "[k]nown and suspected sources of terrorism", to simply "[o]bservation of an individual's behaviour".[41] This Code works to legitimize the use of Schedule 7 by UK authorities, as it restricts who can be investigated, thus reducing the number of interferences with the rights of individuals at ports.

Nevertheless, despite these constraints, there have been several incidents illustrating that there is a severe lack of accuracy and compliance with the governing Code. In July of 2016, Faizah Shaheen was detained by the British Police under Schedule 7 after being reported two weeks earlier for reading a book entitled; "Syria Speaks: Art and Culture from the Frontline".[42] In October of that year, a 35 year old man was detained, arrested, and forced to hand over his unlocked phone under Schedule 7, following his decision to book a different airline for his trip back from a family holiday in Turkey.[43] A year later in October 2017, Eleanor Jones was detained in Edinburgh Airport, solely on the basis that she was part of a campaign against the impact of globalization.[44] These examples illustrate the disparity between the stated aims of the Code of Practice and the reality of police action in the United

[39] s2(4) Schedule 7 Terrorism Act 2000
[40] Paragraph 19, Examining Officers and Review Officers under Schedule 7 to the Terrorism Act 2000, Code of Practice, Home Office, March 2015 (last updated 17 March 2016)
[41] Ibid.
[42] *British woman held after being seen reading book about Syria on plane*, Sian Cain, The Guardian, 4th August 2016, Accessed via https://www.theguardian.com/books/2016/aug/04/british-woman-held-after-being-seen-reading-book-about-syria-on-plane on 25/11/17
[43] *Met police investigating Muslim man's wrongful arrest over terrorism*, Diane Taylor, The Guardian, 3rd April 2017, Accessed via https://www.theguardian.com/uk-news/2017/apr/03/met-police-investigating-muslim-man-wrongful-arrest-terrorism on 25/11/17
[44] *Eleanor Jones claims she was treated like a terrorist by Police Scotland*, Paul Hutcheson, The Herald, 15th October 2017, Accessed via http://www.heraldscotland.com/news/15597078.Revealed__how_Police_Scotland_treated_a_political_activist_like_a_terrorist/ on 25/11/17

Kingdom. Therefore, it is of little surprise that there have been several cases before the domestic courts questioning whether this legislation is in line with fundamental rights.

One of the most high profile challenges to Schedule 7 concerned David Miranda, who was detained at Heathrow Airport in 2013 on the basis that he was carrying electronic information relating to the US whistle-blower, Edward Snowden.[45] He consequently argued that this was a disproportionate interference with his rights under Articles 5, 8, and 10 of the ECHR.[46] Following a dismissal of his claim at the High Court, he sought a reversal from the Court of Appeal, who held that although a mental element was required for justifications under the ground of terrorism, this was fulfilled in the appellant's case.[47] However, the Court also found that the stop powers authorized by Schedule 7 lacked proper judicial safeguards, thereby failing to meet the "prescribed by law" requirement of Article 10(2) ECHR.[48] Where this power is utilised to obtain journalistic material, it was held that the Convention required there to be "sufficient legal safeguards to avoid the risk that power will be exercised arbitrarily and thus that unjustified interference with a fundamental right will occur".[49] The lack of independent and immediate judicial oversight, combined with the high level of protection given to journalistic sources by Article 10, meant that Schedule 7 could not be interpreted as being in line with the ECHR.[50]

Many commentators and civil liberties advocates viewed this decision as a victory for human rights, as it recognised the definitive weaknesses and issues with the scope and

[45] *Terrorism Act incompatible with human rights, court rules in David Miranda case*, Owen Bowcott, The Guardian, 19th January 2016, Accessed via https://www.theguardian.com/world/2016/jan/19/terrorism-act-incompatible-with-human-rights-court-rules-in-david-miranda-case on 30/11/17
[46] *R (David Miranda) v. Secretary of State for the Home Department*, [2016] EWCA Civ 6, at [21]
[47] Ibid., at [55]
[48] Ibid., at [115]
[49] Ibid., at [94]
[50] Ibid., at [113]

structuring of the legislation.[51] However, the Court's decision only struck at very specific circumstances: where the information sought to be obtained is covered by the journalistic privilege. Whilst this does mark a step forward in human rights adherence, the major structural problems of Schedule 7 remain, especially in regards to the forced disclosure of electronic data. For example in 2017 Muhammad Rabbani, the director of the advocacy group CAGE, was detained at Heathrow Airport and ordered to hand over the passwords to his mobile phone and laptop.[52] Mr. Rabbani had been visiting a client in Qatar who claimed to have been tortured in the United States, and thus he had several pieces of confidential evidence about this case on his devices.[53] Accordingly, he refused to comply with the disclosure order, and was then arrested for "wilfully obstructing a stop-and-search under Section 7 of the Terrorism Act".[54] Following his conviction, his lawyers indicated that they wished to appeal to the High Court on the basis that the powers granted to authorities under Schedule 7 do not adequately protect private or legally privileged information.[55] Whilst this appeal was rejected by the High Court in May 2018, Mr Rabbani has "vowed to appeal to the Supreme Court".[56] At the time of writing, this appeal is yet to be granted.

iii) Germany

Whilst UK courts appear to have cemented their jurisprudence in favour of key disclosure, the position emanating from their German counterparts is in every way the antithesis. This form of compulsion would simply not fit with the fundamental principles that

[51] *Terrorism Act incompatible with human rights, court rules in David Miranda case,* Owen Bowcott, The Guardian, 19th January 2016, Accessed via https://www.theguardian.com/world/2016/jan/19/terrorism-act-incompatible-with-human-rights-court-rules-in-david-miranda-case on 30/11/17

[52] *Campaign group chief found guilty of refusing to divulge passwords,* Owen Bowcott, The Guardian, 25th September 2017, Accessed via https://www.theguardian.com/uk-news/2017/sep/25/campaign-group-director-in-court-for-refusing-to-divulge-passwords on 30/11/17

[53] Ibid.

[54] Ibid.

[55] Ibid.

[56] *Cage director Rabbani heads for Supreme Court after appeals court rules password demands lawful*, B Goodwin, Computer Weekly, 15th May 2018, Accessed via https://www.computerweekly.com/news/252441125/Cage-director-Rabbani-heads-for-Supreme-Court-after-appeals-court-rules-password-demands-lawful on 24/10/2018

underlie the German legal system, due to their strong beliefs in encryption and privacy, making Germany one of the most "pro-crypto" nations in the world.[57] For example, in 1999 the German Federal Ministry for the Interior released a document entitled "Cornerstones of German Encryption Policy", through which they aimed to make Germany the "no.1 encryption location".[58] As noted by the Open Technology Institute, "[t]he absence of encryption backdoors, compulsory key disclosure, or mandatory decryption laws is a direct consequence of Germany's unique conception of privacy, strongly informed by its Nazi history and East Germany's experiences under Stasi surveillance".[59] As a result, the particular circumstances of Germany's history have prevented them from following the lead of countries such as the United Kingdom in decreasing protection of citizens' encryption over time.

However, in recent years this dedication has begun to waver.[60] In 2015, Thomas de Maizière, the former Federal Minister for the Interior, in a response to the Charlie Hebdo attacks, requested that the Government be able to "decrypt or bypass encrypted communication".[61] A similar rhetoric was followed in February 2017, where in a joint letter with the French Interior Minister, Mr de Maizière proposed new EU legislation permitting authorities to decrypt information in instances of crime.[62] Later that year, the German Government amended the Code of Criminal Procedure, Section 100a of which now permits the installation of a "state trojan" onto a suspect's device, allowing authorities to bypass any

[57] K Banston & R Schulman, *Deciphering the European Encryption Debate: Germany*, New America, July 11th 2017, Open Technology Institute, pg. 5
[58] *Bundesinnenministerium: "Eckpunkte der deutschen Kryptopolitik" von 1999 haben immer noch Bestand*, M Monroy, Netz Politik, 17th June 2015, Accessed via https://netzpolitik.org/2015/bundesinnenministerium-eckpunkte-der-deutschen-kryptopolitik-von-1999-haben-immer-noch-bestand/ on 28/01/18
[59] K Banston & R Schulman, July 11th 2017, Open Technology Institute, pg. 9
[60] Ibid., pg. 10
[61] *The Encryption Debate We Need*, T Benner, M Hohmann, Global Public Policy Institute, 19th May 2016, Accessed via http://www.gppi.net/publications/data-technology-politics/article/the-encryption-debate-we-need/?L=0&cHash=9c0a6af9c1c08dc958640ccf396b76b6 on 28/01/18
[62] K Banston & R Schulman, July 11th 2017, Open Technology Institute, pg. 6

encryption key, and directly access communications.[63] This law authorises German investigators to access the same amount of electronic information as their UK counterparts, however they do so without any cooperation from the suspect. Although the exact same result is achieved, the lack of cooperation in the instance of Germany means that the two legal procedures have completely different interactions with criminal procedure rights. It is very likely that Germany's trojan law will infringe citizen's right to privacy, or potentially the presumption of innocence, as will be discussed in later chapters. However, due to the adherence to the *nemo tenetur* principle, their legislation will not interfere with the privilege under the right to a fair trial.[64]

This difference in approach can be further illustrated through a study of Germany's laws on search and seizure. Sections 94 and 95 of the German Code of Criminal Procedure prescribe that any "objects which may be of importance as evidence for the investigation" must be surrendered by the accused under threat of fine or criminal sanction.[65] These provisions would appear to encompass the forced release of a password, however, quite crucially, Section 95 is qualified by its final words of "[t]his shall not apply to persons who are entitled to refuse to testify".[66] Thus, those who refuse to comply will not face the sanctions prescribed in Section 70.[67] The inclusion of this sentence is mandated by both the right to personality in the German Basic Law, and more specifically, Section 136 of the Code of Criminal Procedure, which provides the privilege against self-incrimination.[68] It is this privilege that separates the fair trial compatibility of the two jurisdictions' provisions, as even

[63] *New surveillance law: German police allowed to hack smartphones*, C Bleiker, DW, 22nd June 2017, Accessed via http://www.dw.com/en/new-surveillance-law-german-police-allowed-to-hack-smartphones/a-39372085 on 28/01/17, s100a The German Code of Criminal Procedure, StPO
[64] J Gesley, *Government Access to Encrypted Communications*, The Law Library of Congress, May 2016, pg. 36
[65] s94, 95, The German Code of Criminal Procedure, StPO
[66] Ibid., s95
[67] Ibid., s70
[68] Article 2 Basic Law for the Federal Republic of Germany, s136(1) The German Code of Criminal Procedure, StPO

if German lawmakers were to advance their desire to access encrypted information, this restriction means that they will be far more likely to continue with attempts that do not require the suspect's interaction.

Nonetheless, it is by no means a certainty that the issue of key disclosure would be regarded by both domestic and international courts to violate the right against self-incrimination. Indeed, as previously mentioned, the UK Court of Appeal held in *R v. S and Another* that the privilege was not engaged.[69] Jurisprudence from the United States has also 'muddied the water' on this conflict, where there have been several contrasting opinions on whether compelling the release of a password is unconstitutional under the Fifth Amendment.[70] Therefore, it is necessary to analyse the privilege against self-incrimination, in respect of both its rationales and exceptions, in order to conclude whether key disclosure laws can be said to violate criminal procedure rights. This analysis will be performed though a study of the jurisprudence of the European Court of Human Rights, which despite having not heard a case directly on this issue, provides the most wide ranging, and at times contradictory, views on the scope of the privilege.

iv) The Privilege against Self-Incrimination

Whilst the laws regulating key disclosure are of recent development, the privilege against self-incrimination's origins reach back hundreds of years. Some commentators place its conception in the English common law in 1641, following the abolishment of the Star Chamber and the "Ex Officio" procedure, under which the accused was forced to answer all questions under oath.[71] However, others date it much further in the past. For example, in a 4th Century commentary on a letter by Saint Paul, Saint John Chrysostom stated that "I do not

[69] See page 11 above.
[70] See *In Re Boucher* WL 424718 (2009). *United States v. Kirschner*, 823 F. SUPP. 2d 665 (2010).
[71] J D Jackson, S J Summers, *The Internationalisation of Criminal Evidence: Beyond the Common Law and Civil Law Traditions*, Cambridge, 2012, pg. 241

say to you that you should betray yourself in public nor accuse yourself before others, but that you obey the prophet when he said, 'Reveal your ways unto the Lord'".[72] As noted by Helmholz, this extract formed the basis of the legal principle of *nemo tenetur de tegere turpitudinem suam*, namely, that "no one is compelled to bear witness against himself, because no one is bound to reveal his own shame" or to betray himself in public.[73] The privilege later formed part of the European *ius commune,* where no one could be required to "be the source of their own prosecution".[74] More modern conceptions of the privilege have not strayed far from these foundations, such as the English Criminal Evidence Act 1898, which states that "a person charged in criminal proceedings shall not be called as a witness in the proceedings except upon his own application".[75] The United States Constitution offers a more coherent definition in its Fifth Amendment, where it proclaims, "[n]o person…shall be compelled in any criminal case to be a witness against himself".[76] These formulations struck primarily at the trial stage, preventing the compelled questioning of the accused in a court. It is currently estimated that 48 constitutions provide a right against self-incrimination, with over half limited to in trial protection.[77] However, it is clear from the present discussion that the privilege must extend beyond this limitation and encompass pre-trial questioning, and various jurisdictions have already followed such a broader interpretation.[78]

A further distinction must be made between two terms often nonchalantly used to describe this protection; the "privilege against self-incrimination" and the "right to silence". As noted by Treschel, despite many using these guarantees interchangeably, they are better represented as "two overlapping circles".[79] Whilst both rights will prevent certain evidence

[72] R H Helmholz et al, *The Privilege Against Self-Incrimination*, Chicago, 1997, pgs. 1, 26
[73] Ibid.
[74] J D Jackson, S J Summers, Cambridge, 2012, pg. 241
[75] s1(1) Criminal Evidence Act 1898
[76] 5th Amendment, The Constitution of the United States
[77] J D Jackson, S J Summers, Cambridge, 2012, pg. 242
[78] For example see s136 The German Code of Criminal Procedure, StPO.
[79] S Treschel, *Human Rights in Criminal Proceedings*, Oxford, 2005, pg. 342

being used against an accused, the "right to silence" will cover only acoustic declarations, whilst the "privilege against self-incrimination" is limited to preventing the use of information that is incriminating.[80] For our present purposes, it is not instantly clear which formulation is the most appropriate in analysing the human rights compliancy of key disclosure. On one hand, the right to silence may not encompass every case covered, as in addition to being forced to speak out their passwords, suspects may be compelled to enter them directly into their devices. However, the privilege against self-incrimination also has its limits for this study, as the disclosure of a password to an electronic device will not always be *per se* incriminating.

Fortunately, the ECtHR have been expansive with their own interpretation of this right, meaning that it may cover both of the aforementioned situations. In their analysis, they have often referred to the protection as "the right not to incriminate oneself", whilst at the same time categorizing it as being "primarily concerned" with "respecting the will of an accused person to remain silent".[81] Nevertheless, the privilege was historically not protected by the Council of Europe, as despite its recognition in various national jurisdictions at the time of the ECHR's drafting, it was not included as part of the Article 6 right to a fair trial. Furthermore, when the Council implemented the rights of the accused into the Convention under the Seventh Protocol, they considered adding the privilege but explicitly chose not to.[82] It was not until the case of *Funke v. France* in 1993 that the Court first made steps into providing protection against interferences of this nature.[83] This case concerned the fining of the applicant for failing to produce bank statements on request of customs officers in Strasbourg.[84] In the applicant's submissions to the Court, he argued that this violated his

[80] Ibid.
[81] *Saunders v. The United Kingdom*, Application no. 19187/91, 1996, § 69
[82] D J Harris et al, *Law of the European Convention on Human Rights*, 2nd Edition, New York, 2009, pg. 259
[83] *Funke v. France*, Application no. 10828/84, 1993
[84] Ibid., §12

Article 6(1) right, which he claimed covered the "right not to give evidence against oneself", a principle established in the "legal orders of the Contracting States and in the European Convention and the International Covenant on Civil and Political Rights".[85] The Court agreed with this reasoning, and found a violation on the grounds of the "right of anyone "charged with a criminal offence"…to remain silent and not to contribute to incriminating himself".[86]

In the years since this decision, the Court's understanding of the privilege has remained based on this holding, however the tests used for the finding of a violation have evolved, constituting various separate criteria. Firstly, it must be shown that the applicant is subject to a "criminal charge".[87] The term has an autonomous meaning within the ECHR, under which the individual must be charged with a criminal offence, but this may also be extended to situations where the applicant has not yet been technically charged within the domestic law system.[88] Furthermore, the information or evidence obtained does not necessarily have to be incriminating.[89] The Court clearly set out the primary situations in which the privilege would be engaged in *Weh v. Austria*.[90] For example, the authorities may seek to compel an accused for "the purpose of obtaining information which might incriminate the person concerned in pending or anticipated criminal proceedings against him".[91] This is comparable to the aforementioned Second 49 orders issued under the Regulation of Investigatory Powers Act.[92] The privilege is also engaged in "cases concerning the use of incriminating information compulsorily obtained outside the context of criminal proceedings

[85] Ibid., § 41
[86] Ibid., § 44
[87] Ibid.
[88] J D Jackson, S J Summers, Cambridge, 2012, pg. 250
[89] D J Harris et al, New York, 2009, pg. 264
[90] *Weh v. Austria*, Application no. 38544/97, 2004, § 41
[91] Ibid., § 42
[92] See page 10 above.

in a subsequent criminal prosecution".[93] This could include information obtained in customs proceedings, such as in *Funke v. France.*[94]

Secondly, when considering the level of compulsion needed to infringe Article 6, the resounding consensus from the jurisprudence of the Court is that it must be "in defiance of the will of the accused".[95] Within this, the issue of compulsion is split into two distinct formulations: direct, and indirect. Direct compulsion encompasses the traditional form of forced statements, whereas indirect covers situations where the authorities inform an individual that adverse inferences may be taken from their silence, such as in the case of *John Murray*.[96] However, what is clear in both cases is that the compulsion must be improper.[97] In the recently decided case of *Ibrahim*, the Grand Chamber set out the three principal situations in which concerns of improper compulsion would be brought about.[98] They are as follows; where the accused is "obliged to testify under threat of sanctions"; where "psychological or physical pressure" is employed in order to "obtain real evidence or statements"; and where "subterfuge" is used to gain information.[99] This illustrates both the breadth of the modern formulation of the privilege by the ECtHR, and the vast disarray in interpretations that can follow from it.

The confusion surrounding the right is further depicted in the various interpretations of its "rationale". Two rationales for the privilege against self-incrimination are often provided by the ECtHR, both of which come with limitations for persons subject to key disclosure orders.[100] The first, and perhaps most obvious, rationale is that the privilege serves

[93] *Weh v. Austria*, Application no. 38544/97, 2004, § 43
[94] *Funke v. France*, Application no. 10828/84, 1993
[95] *Saunders v. The United Kingdom*, Application no. 19187/91, 1996, § 68
[96] *John Murray v. The United Kingdom*, Application no. 18731/91, 1996
[97] *Ibrahim and Others v. The United Kingdom*, Application no. 50514/08, 2016, § 267
[98] Ibid.
[99] Ibid.
[100] J D Jackson, S J Summers, Cambridge, 2012, pg. 267

the aim of respecting the will of an accused person to remain silent.[101] This was explicitly stated by the Court in *Saunders v. the United Kingdom* as the primary concern of the right.[102] Other formulations from the Court have expanded upon this rationale, stating that it is based on the premise that the "prosecution in a criminal case seek to prove their case against the accused without resort to evidence obtained through methods of coercion or oppression in defiance of the will of the accused".[103] As this interpretation flows directly from the original purpose of the right, it has been the most commonly replicated among other jurisdictions. For example, the rationale for the right given by the United States Supreme Court, as illustrated in *Murphy v. Waterfront Commission,* is that the privilege reflects the "unwillingness to subject those suspected of crime to the cruel trilemma of self-accusation, perjury or contempt".[104] However, as previously noted, the right to silence differs from the privilege, and this rationale focuses primarily on the former. This has particular complications for the issue of key disclosure, as often the individual will be compelled to enter the password directly into the device, without saying anything. It is possible that a court could view any compelled action as 'breaking silence', yet the current jurisprudential norms arising from various jurisdictions do not appear to lean towards such an expansive interpretation.

The second rationale offered by the Court is that by preventing individuals from being compelled to speak, the privilege consequently reduces any instances of miscarriage of justice. This was the primary rationale given by the Court in *John Murray*, where the Chamber stated that "[b]y providing the accused with protection against improper compulsion by the authorities these immunities contribute to avoiding miscarriages of justice and to securing the aims of Article 6".[105] Of all the rationales provided by the Court, this

[101] S Treschel, *Human Rights in Criminal Proceedings*, Oxford, 2005, pg. 347
[102] *Saunders v. The United Kingdom*, Application no. 19187/91, 1996, § 69
[103] *Jalloh v. Germany*, Application no. 54810/00, 2006, § 100
[104] *Murphy v. Waterfront Commission of N.Y. Harbour*, 378 US 55 (1964)
[105] *John Murray v. The United Kingdom*, Application no. 18731/91, 1996, § 45

finds its roots closest to Article 6, not only through the wording of the *John Murray* judgement, but also in its refection of the presumption of innocence. However, it is also the most limited, especially in regards to protection from laws permitting key disclosure. If the accused individual complies with the authorities request to access their electronic device, their incriminating act cannot lead to a miscarriage of justice. Either they tell the correct password, in which they will indeed confirm themselves to be the owner of the device, or they will provide an incorrect password, in which case the authorities will not be able to get in. In both circumstances, there is no possibility of false information being presented at trial. This thereby aligns itself with DNA, blood, and breath samples under this rationale, as they are all forms of evidence that can only be used to verify another source. As will be discussed below regarding the case of *Saunders*, this may prevent a violation of Article 6 being found in all cases of compelled password disclosure.[106]

The primary issue with the rationales offered by the Court is that neither are flexible enough to offer adequate protection to individuals in the context of modern criminal investigation. They are firmly based on the historical origins of the privilege, under which the only evidence that could be compelled by the police was either spoken, or handed over in physical form. This is simply not sufficient for the information that is currently held by new technology. As noted by Chief Justice Roberts in a 2014 decision of the US Supreme Court, due to the capabilities and information stored in modern phones, "they could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers".[107] The amount of incriminatory evidence held on a phone is thus very likely to supersede any other storage device, and the fair trial protection given should perhaps be the strongest. Nevertheless, it is an issue that has scarcely been considered

[106] See page 30 below.
[107] *Riley v. California*, 134 S. Ct. 2489 (2015)

by domestic and international courts. Therefore, a speculative analysis of the ECtHR's future jurisprudence is required.

v) Interaction between Key Disclosure and Self-Incrimination

As noted in the case of *Heaney and McGuinness,* the right not to incriminate oneself and the right to silence are "not absolute rights".[108] This was partially expanded in *O'Halloran and Francis,* where the Grand Chamber stated that even where the accused is directly compelled to make an incriminating statement, this will not "automatically result in a violation" of Article 6.[109] As a result of this, the ECtHR has developed various detailed exceptions to the privilege. Whilst the compulsory disclosure of a password may result in a violation, this is not assured in every circumstance, and will likely be determined on a case-by-case basis. Therefore, it is prudent at this stage to determine the situations in which the Court would be expected to find a violation of Article 6, and those where one of the exceptions will come into play.

Let us first imagine a scenario where an individual is suspected of committing a minor drug offence. Following a speculative arrest, and the informing of their right to silence, the police instruct them that they are obliged to disclose the code to their mobile phone, and that a failure to comply will result in further criminal sanctions. Through fear of facing further punishment, the accused agrees. On the phone, the police discover text conversations under which the accused has openly admitted to selling drugs, and location data that proves their interaction with a well-known drug supplier. This evidence is then relied on by the prosecution at trial to impose a heavier sentence on the accused. It is clear that in this situation the accused has been unlawfully deprived of his Article 6(1) right. As with the applicant in *Funke*, he has been compelled to "provide the evidence of offences he had

[108] *Heaney and McGuinness v. Ireland*, Application no. 34720/97, 2000, § 47
[109] *O'Halloran and Francis v. The United Kingdom,* Application no. 15809/02, 2009, § 53

allegedly committed".[110] The information has been obtained against his will, and he has been forced to reveal the contents of his mind. Whilst the use of the evidence at trial increases the gravity of the violation, it is not crucial, as the fact that he was charged with a criminal offence is enough to bring the privilege into consideration.[111]

This may change if we imagine that instead of being arrested for a minor drug offence, the accused was instead suspected of child abuse. They are still compelled to reveal their password, and instead of messages, the police find indecent photographs of the applicant with children. The actions of the police have remained the same, and all that has changed is the criminal offence of the accused. Nevertheless, under the jurisprudence of the ECtHR, this makes a significant difference. In the case of *Jalloh v. Germany*, the Grand Chamber crucially stated that in determining "whether the proceedings as a whole have been fair, the weight of the public interest in the investigation and punishment of the particular offence in issue may be taken into consideration and be weighed against the individual interest that the evidence against him be gathered lawfully".[112] Later in the judgement, the Court used this qualification as part of a test for determining whether there had been a violation of the privilege. In addition to the public interest consideration, the Court took regard of the "nature and degree of compulsion used to obtain the evidence", the "existence of any relevant safeguards in the procedure" and the "use to which any material so obtained is put".[113] The Court deemed that the public interest in securing the applicant's conviction was low, as he was a minor drug dealer, which alongside the finding of Article 3 violation in regards to the compulsion, amounted to an infringement of the privilege.[114] In the current circumstances, the Government could argue that the public interest in securing the applicant's conviction

[110] *Funke v. France*, Application no. 10828/84, 1993, § 44
[111] See page 23 above.
[112] *Jalloh v. Germany*, Application no. 54810/00, 2006, § 97
[113] Ibid., § 107
[114] Ibid., §§ 107, 118

was of the highest degree, thereby outweighing the nature of the compulsion. However, the Court made clear in the case of *Heaney and McGuinness* that public order and security concerns "cannot justify a provision which extinguishes the very essence of the applicants' rights to silence and against self-incrimination".[115] The applicants in that case had been, in a similar manner to the present situation, threatened with a criminal sanction if they remained silent.[116] This was deemed to destroy the "very essence" of the right, and thus the public interest could not be taken into account.[117] Therefore, it is likely that a violation of Article 6 would be found in this case once again.

International jurisprudence on the privilege opens the possibilities of further expansions of the tests applicable to key disclosure. For example, the conclusion may change if we imagine that upon arresting the individual, his phone was found open, displaying the indecent photographs on the screen. Following taking the suspect to the police station, the phone switched to standby, meaning that the police could no longer access the photographs without the encryption key from the individual. Under US law, this situation would fall under the "forgone conclusion" doctrine, first set out by the Supreme Court in the case of *Fisher v. United States*.[118] Where the authorities already know the "existence and location" of the evidence, the Court has held that forcing the accused to produce this information will be constitutional.[119] Furthermore, as explained in the subsequent case of *Hubbell*, this would only need to be known with "reasonable particularity".[120] However, it is the Vermont District Court's decision of *In re Boucher* that provides the strongest evidence for the outcome of this situation.[121] In that case, the defendant was stopped on the Canadian border by a customs

[115] *Heaney and McGuinness v. Ireland*, Application no. 34720/97, 2000, § 58
[116] Ibid., § 10
[117] Ibid., §§ 55, 58
[118] *Fisher v. United States*, 425 U.S. 411 (1976)
[119] Ibid.
[120] *United States v. Hubbell*, 530 U.S. 27 (2000)
[121] *In re Boucher*, WL 424718 (2009)

officer, who then discovered an open laptop with over 40,000 images appearing to contain child pornography.[122] After copying the laptop's hard drive, the authorities could no longer access the images as they were protected by an encryption key.[123] Due to the foregone conclusion doctrine, compelling the defendant to unlock the images was held to be constitutional, as the Government knew of the existence and location of the files.[124] This principle is yet to find a counterpart in the jurisprudence of the UK, Germany, or the ECtHR, however some commentators have argued that it can possibly be read into the *Funke* judgement.[125] The Court in *Funke* noted that the authorities forced the applicant to provide "documents which they believed must exist, although they were not certain of the fact".[126] This appears to suggest that if the authorities knew the existence of the documents, then the Court may have created an exception. Nevertheless, a case of such facts is yet to reach Strasbourg.

There is one primary exception offered by the ECtHR that is yet to be discussed, which could lead to a finding of no violation in all of the above scenarios. In the case of *Saunders*, the Court stated that the privilege did not extend to "material which may be obtained from the accused through the use of compulsory powers but which has an existence independent of the will of the suspect".[127] This principle, referred to from here on as the *Saunders* exception¸ was created to permit the compulsory collection of evidence that could be taken without the cooperation of the suspect, such as "documents acquired pursuant to a warrant, breath, blood and urine samples, and bodily tissue for the purpose of DNA testing".[128] This prevents Article 6 from interfering with actions that are strictly necessary for

[122] Ibid.
[123] Ibid.
[124] Ibid.
[125] B Koops, *Commanding Decryption and the Privilege Against Self-Incrimination*, Tilburg, 2000, pg. 7
[126] *Funke v. France*, Application no. 10828/84, 1993, § 44
[127] *Saunders v. The United Kingdom*, Application no. 19187/91, 1996, § 69
[128] Ibid.

criminal investigations, such as the matching of a suspect's fingerprints, or the testing of breath for alleged drunk driving. As noted above, the UK Court of Appeal held in the case of *R v. S and Another* that encryption keys should also be deemed to exist independently of the will of the suspect.[129] In their reasoning, the Court noted that once the encryption key was created, it existed as a piece of information independent of the suspect's mind, and would be the equivalent to "the key to a locked drawer".[130] The Court further linked the password to the *Saunders* exception, stating that "[i]n much the same way that a blood or urine sample provided by a car driver is a fact independent of the driver, which may or may not reveal that his alcohol level exceeds the permitted maximum, whether the defendants' computers contain incriminating material or not, the keys to them are and remain an independent fact".[131] It was noted that if the material gained was incriminating, then the privilege might be engaged, however, in those circumstances it would be up to the trial judge to exclude the evidence.[132] Due to the status of passwords under the *Saunders* exception, the act of key disclosure would be no more incriminatory than accessing documents pursuant to a warrant.

This interpretation of the compatibility of key disclosure orders is yet to be tested before the Strasbourg Court. Indeed, the closest the Court has got to a position on this was in the *Saunders* judgement itself. In his dissenting opinion, Judge Martens expressed his apprehension to both the decision of the Court in finding a violation of Article 6, and their construction of the aforementioned exception.[133] He argued that the distinction between the permitted material and incriminating data was not clear, as "in both cases the will of the suspect is not respected in that he is forced to bring about his own conviction".[134]

[129] *R v. S & Anor,* [2008] EWCA Crim 2177 at [20]
[130] Ibid.
[131] Ibid., at [21]
[132] Ibid., at [24] – [25]
[133] Ibid., Dissenting Opinion of Judge Martens joined by Judge Kruis, §§ 1, 12
[134] Ibid.

Specifically, he questioned the compatibility of a "PIN code or a password into a cryptographic system which are hidden in the suspect's memory".[135] Whilst it can be claimed that a dissenting opinion written twenty-two years ago should not be taken as the authorising ECtHR opinion on this issue, it remains the only evidence available. This in itself constitutes the problem. The Court's jurisprudence on the privilege against self-incrimination is severely dated, leaving gaps in its own case law, and a lack of direction for the judiciaries of the Contracting States. The vast number of different results based on minor changes in circumstance means that it will be very difficult to provide a strong set of principles on key disclosure, unless the ECtHR decides to either allow, or prohibit, the practice in its entirety.

vi) The Particular Issues Presented by New Technologies

Up until late 2013, this would have been the endpoint of the analysis. However, the release of the Apple iPhone 5S, and 2017's iPhone X, have potentially altered the entire future relationship between password disclosure laws and the privilege against self-incrimination.[136] In September 2013, Apple released the iPhone 5S under the caption of "the most forward thinking smartphone in the world", with the primary advertising revolving around their new "Touch ID Fingerprint Sensor".[137] This new feature permitted users to replace their standard key code or password with their fingerprint, which they could use to purchase items, authorise downloads, and more crucially, unlock the phone.[138] Whilst this form of technology had previously been available on other devices, it was not until the release of this phone that it truly hit the world market.[139] It is now suggested that there are

[135] Ibid.
[136] *History of the iPhone 2007 – 2017: the journey to the iPhone X*, D Grabham, T3, 10th January 2018, Accessed via https://www.t3.com/features/a-brief-history-of-the-iphone on 06/02/18
[137] *Apple Announces iPhone 5s – The Most Forward Thinking Smartphone in the World*, Press Release, Apple, 10th September 2013, Accessed via https://www.apple.com/newsroom/2013/09/10Apple-Announces-iPhone-5s-The-Most-Forward-Thinking-Smartphone-in-the-World/ on 06/02/18
[138] Ibid.
[139] K Goldman, *Biometric Passwords and the Privilege against Self-Incrimination*, 33 Cardozo Arts & Ent. L. J. 211, 2015, pg. 215

over 700 million iPhone users worldwide, and although a percentage of these may be pre-touch ID versions, phones from Motorola, HTC, and Samsung now additionally offer this feature.[140] The purpose of this paper is not to question the reasons behind this development, however it is clear that this new function has completely changed the position of fingerprints in criminal investigation. When the principles and exceptions of self-incrimination were construed by domestic and international courts, fingerprints were largely seen as nothing more than an indication of identity, and not a key to unlock a wealth of incriminating evidence.[141] Consequently, what has been sold as a strong form of securing personal data has instead weakened the user's access to fundamental rights protection. As noted by TIME magazine, due to the current structure of the privilege, "data protected only by an old-school passcode is afforded stronger legal protection".[142] There are further suggestions that Apple have been made aware of this situation, after the recent iOS 11 operating system provided the so-called "police button", where after pressing the home button five times the touch ID would disable, thereby hiding data from the authorities.[143] Nevertheless, this function's use has not been confirmed by Apple, and it would only protect against the practice of instantly pressing the suspect's finger on their phone, and not a subsequent key disclosure order.

When considering the applicability of passwords to the *Saunders* exception, it was posed that a certain interpretation by the Court could place them in a similar category to physical evidence that has an existence independent of the will of the

[140] *Here's How Many iPhones Are Currently Being Used Worldwide*, D Reisinger, Fortune, 6th March 2017, Accessed via http://fortune.com/2017/03/06/apple-iphone-use-worldwide/ on 06/02/18 , *Fingerprint-scanning phones we have known*, J Dolcourt, CNET, 12th March 2014, Accessed via https://www.cnet.com/pictures/phones-you-can-unlock-with-your-fingerprint-pictures/ on 6/02/18

[141] K Goldman, 33 Cardozo Arts & Ent. L. J. 211, 2015, pg. 231

[142] *Why the Constitution Can Protect Passwords But Not Fingerprint Scans*, J Linshi, TIME, 6th November 2014, Accessed via http://time.com/3558936/fingerprint-password-fifth-amendment/ on 06/02/18

[143] *Apple adds 'police button' to iPhones to protect users from intrusion*, M Bridge, The Times, 19th August 2017, Accessed via https://www.thetimes.co.uk/article/apple-adds-police-button-to-iphones-to-protect-users-from-intrusion-5xz26bx8t on 06/02/18

suspect.[144] This change in technology means that such a move in precedent has become substantially more realistic. As a fingerprint is clearly something that can be taken without the suspect's cooperation or "will", and constitutes physical evidence, the fact that it may also work as a key will be unlikely to render it inside the scope of the privilege's protection. As stated by Andrew Crocker, an attorney at the Electronic Frontier Foundation, the use of a police warrant to access fingerprint passwords is a "clever end-run" around fair trial rights.[145] Whilst there would have to be very specific circumstances for the authorities to lawfully compel the verbal disclosure of a password, pressing an individual's thumb to their phone comes with far fewer legal complications.

This position is supported by jurisprudence originating from US courts, which again are the only judicial bodies to have currently faced this issue. The first case arose in Virginia in 2014, one year after the release of the iPhone 5S.[146] The defendant, Mr. Baust, was arrested for domestic abuse, and the police had strong reason to believe that recordings of the alleged violence were contained on his phone.[147] The authorities sought an order compelling the individual to produce either the passcode or his fingerprint to unlock the encrypted device.[148] The Circuit Court held that whilst the defendant could not be forced to unlock his phone via passcode, he could "be compelled to produce his fingerprint to do the same".[149] This was because the fingerprint, in a similar manner to a key, did not require the defendant to "divulge anything through his mental processes" or to "communicate any knowledge", thereby making the production "non-testimonial" and

[144] See page 30 above.
[145] E Lemus, *When Fingerprints Are Key: Reinstating Privacy to the Privilege against Self-Incrimination in Light of Fingerprint Encryption in Smartphones*, 70 S.M.U. L Rev 533, 2017, pg. 537
[146] *Commonwealth of Virginia v. Baust*, 89 Va. Cir. 267 (2014), pg. 1
[147] Ibid.
[148] Ibid.
[149] Ibid., pg. 4

constitutional.[150] This line of reasoning was confirmed in the subsequent case of *Stahl*.[151] Although this case did not concern touch ID, the District Court of Appeal of Florida stated in obiter dicta that "[c]ompelling an individual to place his finger on the iPhone would not be a protected act; it would be an exhibition of a physical characteristic…not unlike being compelled to provide a blood sample or provide a handwriting exemplar".[152] This holding, akin to the *Saunders* exception, illustrated that it is not only the ECtHR that may fail to understand the new functions of the fingerprint.

Nevertheless, it looked as though a case in Illinois in early 2017 was going to alter not only this line of precedent, but the entire theoretical position on key disclosure.[153] The District Court decided to go beyond the repeated analysis of whether the password was a testimonial or non-testimonial material, and instead based their decision on what evidence could be obtained by its compulsion.[154] The Court stated that they could not equate the "limited protection" given to fingerprints used for identification to "forced fingerprinting to unlock an Apple electronic device that potentially contains some of the most intimate details of an individual's life".[155] From the point of view of the due process model, this is the perfect decision on key disclosure and self-incrimination, and one that would be ideally followed by other domestic and international judiciaries. The Court effectively reacted to the new technology, understanding that they could not apply archaic standards on fingerprints to this situation.

However, a recent decision by the Supreme Court of Minnesota has threatened to undo this progress. In *State v. Diamond*, the Court retracted to the reasoning that the

[150] Ibid.
[151] *State of Florida v. Stahl*, 206 So.3d 124 (2016)
[152] Ibid, pg. 135
[153] *In re Application for a Search Warrant*, 236 F.Supp.3d 1066 (2017)
[154] Ibid.
[155] Ibid., at pg. 1073

fingerprint password did not require the will of the suspect, noting that the defendant "did not even need to be conscious".[156] They further tried to distance the authority's action from the privilege, arguing that it was not placing the defendant's finger on the phone that unlocked it, but instead the phone analysing the fingerprint and matching it with the stored data.[157] This is a short-sighted judgement, which completely ignores the real issue at hand, namely, that by taking the defendant's fingerprint they have access to a great amount of possibly incriminating information.

Judging from the decision in *R v. S and Anor*, it is highly likely that the UK courts would also permit this form of forced decryption.[158] As has been discussed in regards to the *Saunders* principle, if the court has already made the step to accept the compulsion of passwords as lawful, it is of no further effort to expand this to fingerprints. However, a more interesting threat is that which may face citizens' rights in Germany. As previously mentioned, German law does not permit any key disclosure, due to the strong protection given to the privilege against self-incrimination.[159] Nevertheless, the action of placing the suspect's finger on the sensor, despite reaching the same result, is not strictly key disclosure. No order is needed to go through a Court, and it does not involve any exertion from the accused. Whilst Section 136 of the German Code of Criminal Procedure permits the suspect to remain silent, Section 81b authorises the police to take photographs and fingerprints from them, "even against his will".[160] Due to the German judicial system's strong belief in encryption, it is unlikely that they would permit an order to reveal a password, yet the mere obligation to provide a fingerprint may well be not only permissible, but also protected under the Code of Criminal Procedure.

[156] *State of Minnesota v. Diamond*, 2018 WL 443356 (2018), pg. 6
[157] Ibid.
[158] *R v. S & Anor*, [2008] EWCA Crim 2177
[159] See page 18 above.
[160] s81b, 136(1) The German Code of Criminal Procedure, StPO

What is perhaps more concerning for this legal issue is the developments made to passwords by the newest release of smartphones, primarily heralded by the iPhone X. The new function of 'Face ID' permits users to unlock their phone by merely looking at it, made possible by camera technology that captures over 30,000 infrared points on a person's face.[161] In the context of criminal investigation, this would allow the authorities to simply present a phone towards a suspect's face, which would instantly unlock it. Unlike in the cases of the previously described forms of encryption, the suspect will not be compelled to do anything other than be in presence of the police officers. This appears to be the point at which phone passwords may completely evade the privilege. Under the various rationales and tests provided by the ECtHR, this would not amount to a violation of Article 6. The accused can remain silent, and the password undoubtedly exists independent of their will. The new technology offered by phone manufacturers may greatly assist users in the accessibility of their devices, but it will consequently gravely weaken their fair trial rights. Unless the law reacts to these changes, for example as the Court did in *In re Application for a Search Warrant,* then various aspects of the privilege against self-incrimination will become superfluous.[162]

The legal provisions providing the right to silence and the privilege against self-incrimination vary across different jurisdictions, both in regards to their formulations and their exceptions. However, it appears that they all have one thing in common: they are simply not ready to competently address the threat posed by key disclosure orders and modern technology. Legislation such as the UK's Regulation of Investigatory Powers Act and Terrorism Act has created criminal investigatory powers that permit the authorities to access

[161] *Apple's Use of Face Recognition in the New iPhone: Implications*, J Stanley, ACLU, 14th September 2017, Accessed via https://www.aclu.org/blog/privacy-technology/surveillance-technologies/apples-use-face-recognition-new-iphone on 07/02/18

[162] *In re Application for a Search Warrant*, 236 F.Supp.3d 1066 (2017)

a wide range of incriminatory information, without any restrictions from fair trial rights. The narrative arising from the German legislature, despite being grounded in a pro-encryption foundation, is slowly regressing to a similar point, with new amendments permitting intrusions on suspects' private data. The courts in these jurisdictions can find little support from the ECtHR on this issue, as in addition to having no case law of direct relation, there is a lack of coherent and definitive principles on the privilege itself. As has been illustrated in this chapter, the Court's jurisprudence does not provide a conclusive answer as to whether key disclosure orders are compatible with Article 6. Furthermore, recent technological developments have brought additional confusion to the debate, with fingerprint and facial recognition encryption entering the mass smartphone market. Judicial holdings from the United States may help in providing some guidance in this area, however until the ECtHR hear and make a clear judgement directly on this issue, this question will remain unanswered.

Chapter 2: Surveillance and its Impact on the Presumption of Innocence

i) Introduction

Whilst the use of forced key disclosure orders has assisted domestic authorities in gaining access to electronic information directly from the suspects to a crime, it is not always possible, or strategic, to make contact with the individual before charges can be brought. In such situations the police will often resort to surveillance, for obtaining the evidence necessary to bring a prosecution, or to attempt to catch a suspect in the commission of an offence. Traditionally, this investigative technique would require individual officers to photograph a suspect, or to directly intercept their telephone communications. However, due to the aforementioned developments in technology, and the wealth and value of information stored on mobile phones and laptops, investigative surveillance has evolved into a completely different beast. Whereas during traditional surveillance "what the surveillant knows, the subject probably knows as well", in modern practices the "surveillant knows things the subject doesn't".[163] The expansion and reliance by society upon certain forms of technology has left citizens vulnerable to greater invasions of their privacy, to a degree where having electronic information revealed to the authorities is almost an inevitability. As noted by David Lyon, surveillance "has spilled out of its old nation-state containers to become a feature of everyday life, at work, at home, at play and on the move".[164]

Within the United Kingdom and Germany, the issue of Government surveillance has been a constant subject of political and judicial discussion, however it is only in recent years that its effect has truly received widespread public attention. It has been argued that in the post 9/11 climate, 'security' has substituted 'peace' or 'welfare' as the guiding narrative of

[163] C Fuchs et al, *Internet and Surveillance, The Challenges of Web 2.0 and Social Media*, Routledge, 2012, pg. 1

[164] D Barnard-Wills & H Wells, *Surveillance, technology and the everyday,* Sage, 2012, pg. 227

Western politics, and this has been reflected in an increase in surveillance.[165] Furthermore, following the 2013 revelations arising from the whistleblowing of NSA operative Edward Snowden, any public ambivalence towards this practice could no longer be maintained. The so-called 'Snowden files' revealed that the UK Government, and specifically GCHQ, had "one of the most extensive and technologically advanced surveillance systems in the world".[166] Snowden described the UK's surveillance powers as even "more intrusive to people's privacy than has been seen in the US", as it was revealed that GCHQ was collecting information from a staggering amount of individuals' emails, phone messages, Facebook posts, and internet records, irrespective of whether they had been involved in criminal activities.[167] On the other hand, German outrage towards the Snowden leak focused on the actions of the NSA rather than their own Government, after it was revealed that the former had been monitoring the mobile phone of Chancellor Angela Merkel.[168] This controversy led to German citizens knowing more about the operations of the NSA than their own foreign intelligence service, reinforcing the idea of 'German Exceptionalism' which, as will be discussed below, assumes wrongly that Germany is not conducting its own domestic intelligence operations.[169]

Nevertheless following the Snowden leaks, both the United Kingdom and Germany enacted new legislation on surveillance measures, in an attempt to ensure greater transparency to their actions, and thereby gain public support. In 2016 the UK passed the Investigatory Powers Act, which despite being marketed as simply legalising the actions already employed by GCHQ, was described by Snowden as permitting "the most extreme

[165] M Friedewald et al, *Surveillance, Privacy and Security*, Routledge, 2017, pg. 233
[166] F Davis et al, *Surveillance, Counter-Terrorism, and Comparative Constitutionalism*, London, 2014, pg. 152
[167] R S. Waranch, *Digital Rights Ireland Déjà vu?: Why the Bulk Acquisition Warrant Provisions of the Investigatory Powers Act 2016 are Incompatible with the Charter of Fundamental Rights of the European Union*, George Washington International Law Review, 2017, pg. 210
[168] F H Cate & J X Dempsey, *Bulk Collection*, Oxford, 2017, pg. 63
[169] R A Miller, *Privacy and Power*, Cambridge, 2017, pgs. 354, 364. See page 53 below.

surveillance in the history of western democracy".[170] The German Government made a similar legislative step in the same year, which has been claimed by NGOs and journalists to legalise previously unlawful activities, and thus enhance the surveillance capabilities of the intelligence agencies.[171]

As the data gathering operations of these states have become more transparent, they have consequentially faced increasing numbers of legal challenges.[172] Such objections have been almost exclusively based upon the surveillance's impact upon the right to private life, founded in either the ECHR, the European Charter of Fundamental Rights, or their own national constitutions.[173] Although this has been repeatedly shown to be a relatively successful judicial route to take, it is a topic that is already the subject of extensive academic scholarship. Instead, in following from the previous chapter, this analysis will look at the use of this technology in light of fair trial guarantees, in particular, the presumption of innocence. As the evidence obtained from surveillance practices will often be used in the context of a trial, its use will inevitably have an impact on the due process rights of the suspect.[174]

Furthermore, recent developments in the use of surveillance in criminal investigations have raised questions over whether the presumption should also be extended to pre-trial interferences, with particular regard to the threats posed by preventive policing and pre-crime technology. As the policy directives of policing authorities shift towards preventing crime, surveillance powers are used to target the 'general' rather than the 'specific', monitoring the suspects to crimes that are yet to happen in addition to those that already have.[175] The

[170] L Woods, *The Investigatory Powers Act 2016*, European Data Protection Law Review, 2017, pg. 103. Accessed via https://twitter.com/Snowden/status/799371508808302596 on 25/06/18.
[171] S Steiger et al, *Outrage without Consequences? Post-Snowden Discourses and Governmental Practice in Germany*, Heidelberg, 2017, pg. 10
[172] See for example *R (Davis & Watson) v. Secretary of State for the Home Department,* [2018] EWCA Civ 70, *Big Brother Watch and Others v. The United Kingdom*, Application no. 58170/13, 2018
[173] See for example Article 8 ECHR, Article 7 EU Charter of Fundamental Rights.
[174] D Wright & R Kreissl, *Surveillance in Europe*, London, 2015, pg. 287
[175] D Barnard-Wills & H Wells, Sage, 2012, pg. 229

widespread use of personal technology makes such pre-crime monitoring possible, as their storage of location, camera, and text data permits the surveillance of law-abiding and law-breaking citizens alike.[176] It has been argued that both targeted and untargeted surveillance in the pre-crime stage undermines the presumption of innocence, as it treats innocent people like criminal suspects, stigmatising them in the eyes of society.[177] Nevertheless, this is an opinion largely absent from judicial decisions, especially from international human rights courts such as the ECtHR, whose strict interpretation of the presumption rules out any such advance.

Therefore, it must be established the degree to which developments in technology, and the consequential surveillance imposed on such devices, requires legal challenges under the presumption of innocence in addition to those of the right to private life. The movements in various states, including the United Kingdom and Germany, towards a fully surveilling society, monitoring individuals before and after the commission of criminal offences, must be regarded as a threat to the norms that underpin international human rights. However, the best approach to challenging these practices, and the resulting evidential consequences as will be later discussed in the third chapter, still needs to be ascertained.

ii) Surveillance and its Effects

Whilst the effects of surveillance may pose the greatest threat to the civil liberties and due process rights of individuals today, the act of monitoring the activities of citizens is of no modern invention. In the 5th Century, the Chinese military strategist Sun Tzu stated in his treatise *the Art of War* that "it is only the enlightened ruler and the wise general who will use the highest intelligence of the army for purposes of spying and thereby they achieve the great results".[178] From the spy network employed by Roman Emperor Julius Caesar, to the

[176] Ibid., pg. 232
[177] K Hadjimatheou, *The Relative Moral Risks of Untargeted and Targeted Surveillance*, Ethic Theory Moral Practice, 2014, pg. 194
[178] S Tzu, *The Art of War*, Translated by Lionel Giles, Accessed via http://classics.mit.edu/Tzu/artwar.html

"committees of surveillance" of the 18th Century French revolutionary Government, domestic surveillance has remained a constant throughout history.[179] However, it was arguably not until the late 1800's that the 'modern' practices of government monitoring first became a reality. The introduction of the portable camera in the 1880's led a writer in the New York Times to state that "[t]here is little need for hiding cameras nowadays as the public has become accustomed to the bombardment kept up from the pretty little highly-polished boxes".[180] The development of the camera, the phonograph, and the telephone "laid the foundations of mass surveillance", where the authorities could now obtain personal information from suspects without having to make any form of direct contact.[181] Each of these individual new technologies offered new opportunities for communication and data storage, and consequently opened the doors for law enforcement agencies to gain an unprecedented amount of evidence.[182]

The possibilities for surveillance created by these developments were not received positively by all, and during the 20th Century critics in both the literary and scholarly fields illustrated their distaste towards the increased monitoring of civilians. One of the most infamous and re-produced criticisms of the surveillance society came in George Orwell's novel '*Nineteen Eighty-Four'*, which coined the concept of the 'Big Brother', and led to the term 'Orwellian' often being used as a descriptor for state interference.[183] Following this, Michel Foucault built upon Jeremy Bentham's prison model of the panopticon with his social theory of 'Panotpicism' in *Discipline and Punish.*[184] Using the idea of the panopticon as the all-seeing force in society which models citizens towards certain norms, Foucault described

[179] *Roman Empire to the NSA: A world history of government spying*, A Zurcher, BBC News, 1st November 2013, Accessed via https://www.bbc.co.uk/news/magazine-24749166 on 25/07/18
[180] J Lauer, *Surveillance history and the history of new media: An evidential paradigm*, Sage, 2011, pg. 567
[181] Ibid., pg. 568
[182] Ibid., pg. 570
[183] G Orwell, *1984*, London, 1949
[184] M Foucault, *Discipline & Punish: The Birth of the Prison*, New York, 1975, pg. 195

how daily life had been taken over by "panoptical mechanisms", such as the aforementioned technology, which facilitated criminal investigations, sanctions, and other forms of discipline.[185]

However, the modern improvements made to technology in recent decades has been quickly followed by alterations in surveillance theory. For example, Mark Poster has formulated the notion of the "superpanopticon", where the developments of the internet and technology have permitted "a system of surveillance without walls, windows, towers or guards".[186] The creation of the so-called 'web 2.0' has created a platform for the storage, usage, collection and analysis of a large amount of personal data, moving far beyond the surveillance powers possible in the times of Orwell and Foucault's analyses.[187] This has provoked some commentators, such as Haggerty and Lyon, to argue that due to the decentralisation of internet surveillance, the metaphor of the panopticon has become moot, as it fails to give proper consideration to the contemporary surveillance features of information technology and consumerism.[188]

Nevertheless, it is not only legal theory that has struggled to keep up with the developments made in surveillance technology, as judicial decisions and statutory law have also faced conceptual difficulties in regulating this area of state investigation.[189] Therefore, it is necessary to look into the specificities of domestic investigatory practices and legislation to understand the precise human rights issues posed by modern surveillance, and how the presumption of innocence could potentially be used to challenge it.

[185] M Galič et al, *Bentham, Deleuze and Beyond: An Overview of Surveillance Theories from the Panopticon to Participation*, Tilburg, 2017, pg. 16
[186] C Fuchs et al, Routledge, 2012, pg. 1
[187] Ibid., pg. 5
[188] Ibid., pg. 7
[189] N Witzleb, *Emerging Challenges in Privacy Law*, Cambridge, 2014, pg. 206

a) The United Kingdom

Following the passing of the Great Reform Act in the 1830's, and the creation of an accessible postal service, means of communication in the United Kingdom drastically expanded.[190] Whilst this development permitted British citizens to communicate with others around the country at an unprecedented speed and cost, it was also seen by the Government as a valuable opportunity to protect national security.[191] The resulting 'postal espionage crisis' of 1844, where it was revealed that the Government were opening large amounts of letters on security grounds, constituted the first modern UK privacy scandal.[192] Over 170 years later, the same controversies remain at the forefront of the British civil liberties debate, and it is now often commented that "successive UK governments have gradually constructed one of the most extensive and technologically advanced surveillance systems in the world".[193] Recent statistics estimate that there are between four to six million CCTV cameras currently operating in the United Kingdom, amounting to one camera for every eleven citizens, with security services further having the ability to intercept phone calls, emails, and other forms of communication.[194] Furthermore the UK Secret Services, in particular those operating from GCHQ, have taken full advantage of advances in personal technology to exert control over 'national security' threats. This was the subject of the files released by Edward Snowden in 2013, who revealed that UK authorities had access to the NSA's "Prism" surveillance network, allowing GCHQ to collect electronic data without obtaining a legal warrant, as long as it was accessed through an internet provider outside the UK.[195] The

[190] D Vincent, *Surveillance, privacy and history,* History & Policy, 2013, Accessed via http://www.historyandpolicy.org/policy-papers/papers/surveillance-privacy-and-history
[191] Ibid.
[192] Ibid.
[193] F Davis et al, *Surveillance, Counter-Terrorism, and Comparative Constitutionalism,* London, 2014, pg. 152
[194] *One surveillance camera for every 11 people in Britain, says CCTV survey*, D Barrett, The Telegraph, 10th July 2013, Accessed via https://www.telegraph.co.uk/technology/10172298/One-surveillance-camera-for-every-11-people-in-Britain-says-CCTV-survey.html on 30/07/18
[195] *UK gathering secret intelligence via covert NSA operation*, N Hopkins, The Guardian, 7th June 2013, Accessed via https://www.theguardian.com/technology/2013/jun/07/uk-gathering-secret-intelligence-nsa-prism on 02/08/18

Snowden files further disclosed that GCHQ had monitored the computers and phones of delegates to the G20 summits in London in 2009.[196] The culmination of the scandal resulting from these exposés led to a change in legislative policy on intercepted communications, which will be discussed below.[197]

However, until this shift in legislation, the regulatory framework governing surveillance and interception in the UK was set out by the aforementioned Regulation of Investigatory Powers Act 2000 (RIPA). This legislation provides for the "interception of communications", "the carrying out of surveillance", and as was discussed in the previous chapter, the decryption of electronic data protected by passwords.[198] The Act authorises several forms of surveillance, defined as to include "monitoring, observing or listening to persons, their movements, their conversations or their other activities or communications", "recording anything monitored, observed or listened to in the course of surveillance", and "surveillance by or with the assistance of a surveillance device".[199] For any interception of communications, the order must be issued or approved by one of the individuals set out in Section 6(2), and for surveillance operations, it has to be authorised by a member of a local authority or those mentioned under Section 30.[200] For the endorsement of the latter orders, it has to be shown to be necessary in the interests of either "national security", "preventing or detecting crime or of preventing disorder", "the economic well-being of the United Kingdom", "public safety", "public health", or collecting monetary charges payable to the Government, largely reflecting the list set out in Article 8(2) ECHR.[201] Particular controversy arose surrounding the authorisation of surveillance orders by local councils, as it was shown

[196] *GCHQ intercepted foreign politicians' communications at G20 summits*, E MacAskill et al, The Guardian, 17th June 2013, Accessed via https://www.theguardian.com/uk/2013/jun/16/gchq-intercepted-communications-g20-summits on 02/08/18
[197] See page 48 below.
[198] Regulation of Investigatory Powers Act 2000, Introductory Text
[199] Ibid., s48(2)
[200] Ibid., s30
[201] Ibid., s28(3)

that they were carrying out over eleven surveillance operations every day, for the purpose of preventing acts such as dog fouling, smoking, and fly tipping.[202] For example, Midlothian Council were found to have investigated "dog barking", and it was revealed that Alderdale Borough Council used surveillance to establish who was "feeding pigeons".[203] These authorisations were clearly distinct from the advertised purpose of the Act in preventing serious crime and terrorism, leading to criticism from NGOs and politicians alike of the legislation's "petty and vindictive" nature.[204] This led to the amending Protection of Freedoms Act 2012, Section 37 of which imposed a judicial approval on the aforementioned surveillance powers, with the purpose of restricting its use to only "serious offences".[205]

RIPA remained the sole guiding piece of UK legislation on surveillance practices for 14 years, until the decision of the European Court of Justice in the case of *Digital Rights Ireland*, where they invalidated the European Data Retention Directive on the basis of Articles 7 and 8 of the EU Charter of Fundamental Rights. [206] This Directive had obliged Member States to require telecommunications providers to retain users' location and traffic data, and was held by the ECJ to be contrary to the right to respect for private and family life, and the right to protection of personal data.[207] In a reaction to this judgement, the UK Parliament enacted emergency legislation to "ensure that UK law enforcement and intelligence agencies can maintain their ability to access the telecommunications data they need to investigate criminal activity and protect the public".[208] The resulting Data Retention

[202] Big Brother Watch, *The Grim RIPA*, 2010, pg. 1, Accessed via https://www.bigbrotherwatch.org.uk/TheGrimRIPA.pdf
[203] *Revealed: British Councils used Ripa to secretly spy on public*, A Asthana, The Guardian, 25th December 2016, Accessed via https://www.theguardian.com/world/2016/dec/25/british-councils-used-investigatory-powers-ripa-to-secretly-spy-on-public on 13/08/18
[204] *Council spy cases hit 1,000 a month*, G Rayner, The Telegraph, 12th April 2008, Accessed via https://www.telegraph.co.uk/news/uknews/1584808/Council-spy-cases-hit-1000-a-month.html on 13/08/18
[205] s37 Protection of Freedoms Act 2012, House of Commons Debate, Hansard, 1 Mar 2011 : Column 208
[206] *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, Joined Cases C-293/12 and C-594/12, 8th April 2014
[207] R S. Waranch, George Washington International Law Review, 2017, pg. 220
[208] *The Data Retention and Investigatory Powers Bill*, Commons Briefing Paper, House of Commons Library, 16th July 2014, Accessed via http://researchbriefings.parliament.uk/ResearchBriefing/Summary/SN06934

and Investigatory Powers Act 2014 (DRIPA) largely acted to amend the 2000 Act, however it also empowered the Secretary of State to "require a public telecommunications operator to retain relevant communications data", if following the aforementioned purposes set out in Section 22 of the previous legislation.[209] In 2015, the Conservative MP David Davis sought judicial review of DRIPA, on the basis that it was inconsistent with Articles 7 and 8 of the Charter of Fundamental Rights.[210] The High Court held that for a legislative scheme of this kind to be acceptable under EU Law it had to be sufficiently clear, and expressly restricted to serious offences.[211] DRIPA did not meet this standard, and was therefore inconsistent with EU Law.[212] Following an appeal by the Government, the European Court of Justice held that EU Law must be interpreted as precluding national legislation which provided for "general and indiscriminate retention" of data.[213] The Court further stated that EU Law precluded legislation which allowed access to data on a basis that was not restricted to strictly fighting serious crime, and where access was not subject to prior review by a court or an independent administrative body.[214]

However, nearly one month before the delivery of this judgment, the UK passed the Investigatory Powers Act 2016. This Act was created in response to a 2015 report, which illustrated severe concerns at the lack of powers provided to law enforcement agencies to investigate and prevent terrorism.[215] Furthermore, the Act replaced and built upon the surveillance powers of DRIPA, which expired on 31st December 2016, due to a 'sunset

[209] s1(1) Data Retention and Investigatory Powers Act 2014
[210] *R (on the application of Davis) v Secretary of State for the Home Department*, [2015] EWHC 2092 (Admin)
[211] Ibid., para 91
[212] Ibid.
[213] *Secretary of State for the Home Department v Tom Watson*, Joined Cases C-203/15 and C-698/15, 21st December 2016. The ECJ made reference to article 15(1) of Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), as amended by Directive 2009/136/EC, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter of Fundamental Rights of the European Union.
[214] Ibid., para 102
[215] D. Anderson Q.C., *A Question of Trust, Report of Investigatory Powers Review*, London, 2015

clause' in the legislation.[216] Although the purpose of the Investigatory Powers Act 2016 may have mirrored its predecessors, the content of its provisions expanded UK Government surveillance powers to beyond previous recognition, leading critics such as Edward Snowden to call it "the most intrusive and least accountable surveillance regime in the West".[217] Nonetheless, the Act's provisions initially provided some signs of a move in a positive direction. Part Two of the Act, outlining the process for obtaining a warrant for interception, introduced the 'double lock' system, whereby in addition to being signed by the Secretary of State, the warrant must then be approved by a 'Judicial Commissioner'.[218] Furthermore, the Act was heralded for bringing together the broad range of powers apparent in different pieces of legislation, arguably making the system more transparent and increasing the effectiveness of oversight.[219]

However on closer inspection, the apparent positives of the Act do not come to fruition. Firstly, not all of the powers exercised through the Act are subject to the double lock mechanism, most notably the access to retained communications data.[220] Whilst the initial order to the telecommunications company to retain data will require the approval of the Judicial Commissioner, any later requests to obtain this information can be authorised by anyone regarded to be a "designated senior officer".[221] This essentially erodes the previous benefits of the double lock mechanism, as it is this second point of access which arguably constitutes the greater intrusion on the rights of the individual. Secondly, the nature of the assessment by the "Judicial Commissioner" can in itself be questioned, as the law largely

[216] *Cameron announcing emergency surveillance legislation,* Andrew Sparrow, The Guardian, 10th July 2014, Accessed via https://www.theguardian.com/politics/blog/2014/jul/10/cameron-announcing-emergency-surveillance-legislation-politics-live-blog on 14/08/18
[217] *Edward Snowden attacks UK government over investigatory powers bill,* A Gani, The Guardian, 4th November 2015, Accessed via https://www.theguardian.com/world/2015/nov/04/edward-snowden-attacks-tories-over-investigatory-powers-bill on 14/08/18
[218] s23 Investigatory Powers Act 2016
[219] L Woods, *The Investigatory Powers Act 2016*, European Data Protection Law Review, 2017, pg. 103
[220] Ibid., pg. 104
[221] s23, 61 Investigatory Powers Act 2016

restricts their powers to oversight on procedural grounds. Section 23 of the Act dictates that the Commissioner must look into the decision to grant the warrant on the basis of whether it is "necessary on relevant grounds" and proportionate, whilst applying similar standards to that of "judicial review", and having regard to the "general obligations of privacy", in other words, Article 8 ECHR.[222] Although this may appear to be a sufficiently thorough review, the ability of the Commissioner to scrutinise the warrant will be largely dependent on its specificity, to which there are no concrete requirements.

This will be of particular difficulty when it comes to another significant innovation of the Investigatory Powers Act, namely, 'thematic warrants'.[223] A "targeted equipment interference warrant", referred to in the Explanatory Notes as a "thematic warrant", permits UK authorities to access communications data from a suspect's electronic devices.[224] This form of warrant is fairly analogous to those provided by the previous pieces of legislation outlined, however Section 101 of the Act, detailing the subject matter to be examined, expands its scope exponentially. For example the target of this warrant can be extended to any "equipment belonging to, used by or in the possession" of "a group of persons who share a common purpose or who…may carry on, a particular activity"; "equipment in a particular location"; and any "equipment which is being, or may be, used for the purposes of a particular activity or activities of a particular description".[225] The broadness of these terms means that a warrant could be directed to cover all electronic communications devices in a particular area, and the inclusion of "may" in several of the clauses means that the warrant does not need to be based on solid reasons. Furthermore, this Section permits warrants to be phrased in such a way that it would not be possible for the Judicial Commissioner to properly

[222] Ibid, s23
[223] Investigatory Powers Act 2016, Explanatory Notes, pg. 45
[224] s99(2) Investigatory Powers Act 2016
[225] Ibid., s101(1)

attest to their proportionality, as the specific targets of the surveillance would not be ascertained. The same issue arises in regards of the retention of communications data, authorised under Part 4 of the Act, which requires telecommunications operators to retain all their customers 'metadata', encompassing the sender, recipient, time, length, method, and location of communications.[226] In authorising such a warrant, the Secretary of State again must take into account the proportionality of the measure, including "the likely benefits of the notice", and "the likely number of users" affected.[227] However, this analysis, in addition to that of the Judicial Commissioner, will also be without proper regard to the merits, as it would be impossible to assess the proportionality of measures against all persons who belong to a particular telecommunications provider.

By permitting the bulk collection of metadata, without accurately specifying the time, location, or even specific target, these warrants permit government access to future, non-existing, data.[228] This has been rationalised by the United Kingdom as being a necessary adjustment to surveillance laws in light of the growing popularity and accessibility of internet communications, which have rendered traditional targeted acquisition warrants obsolete.[229] Justifications were also provided on the basis of national security needs, with the current Prime Minister Theresa May stating that "if you are searching for the needle in the haystack, you have to have a haystack in the first place".[230] This type of statement is often used to legitimise surveillance, acting alongside the idea that these processes only affect criminals and the 'undesirables' of society, and that if you have nothing to hide, then you have nothing to fear.

[226] Ibid., s87(11). R S. Waranch, George Washington International Law Review, 2017, pg. 226
[227] s88 Investigatory Powers Act 2016
[228] R S. Waranch, George Washington International Law Review, 2017, pg. 227
[229] Ibid., pg. 227
[230] Ibid., pg. 211

However, such justifications can no longer be viewed as viable in the surveillance discourse of the United Kingdom. The Investigatory Powers Act has moved the monitoring practices of the UK authorities from a reactionary to a precautionary position, falling into the aforementioned 'pre-crime' category. Whilst before it could be believed that you would only be subject to surveillance if you were connected to the commission of a criminal offence, the 2016 Act permits monitoring based on only your acquaintances, location, or telecommunications provider. Under this system, innocent people are encouraged to put up with a reduction in their privacy, in order to ensure the safety of society as a whole.[231] These modern technologies permit the constant monitoring of the activities of all individuals at all times, resulting in previously private and unproblematic actions being "suddenly rendered visible and problematized".[232] As noted by Haggerty and Ericson, "surveillance that was once reserved for the suspect or deviant has become extended to cover the majority of the population".[233] Due to the Investigatory Powers Act, the surveillance of an individual's behaviour is no longer directly correlated to their social status or criminal activity. They are monitored solely because they own a mobile phone, tablet, or laptop, and reside within the borders of the United Kingdom. The technology thus erases the distinction between the guilty and the innocent.[234] As argued by Barnard-Wills, "[i]ndividual behaviour and choices can make an individual a legitimate subject of surveillance, but an individual should not become a target through no action of their own, or because of actions over which they have no voluntary control".[235] It is precisely this point where, as will later be discussed, the act of surveillance collides with and infringes the fair trial principle of the presumption of innocence.

[231] D Barnard-Wills & H Wells, *Surveillance, technology and the everyday,* Sage, 2012, pg. 229
[232] Ibid., pgs. 229, 232
[233] Ibid., pg. 230
[234] D Barnard-Wills, *UK News Media Discourses of Surveillance,* The Sociological Quarterly, 2011, pg. 558
[235] Ibid., pg. 562

b) Germany

As previously mentioned, Germany has an entrenched distrust for government surveillance, harbouring back to the mass monitoring performed in East Germany by the Ministry for State Security, and the previous Nazi regime.[236] In reaction to this, German lawmakers established strong constitutional safeguards against interferences with privacy in the Basic Law, seeking to prevent such actions from recurring. This included Article 10, which provides German citizens with a guarantee that the privacy of their "correspondence, posts, and telecommunications shall be inviolable".[237] Furthermore, Article 13 secures that the home shall also be inviolable, and through judicial interpretation, this clause has been extended to also cover the premises of study, work, and business.[238] Privacy rights have also been developed by the German Federal Constitutional Court to create an entirely new guarantee, the "right of informational self-determination", which protects individuals from interferences into personal activities, and grants a degree of autonomy over their own informational data.[239]

The safeguards granted to German citizens under the Basic Law, and advancements made through judicial interpretations, have formed the aforementioned idea of 'German exceptionalism' when it comes to protection from Government surveillance. This is further enforced by legislation and jurisprudence directly restricting telecommunications and data interference by authorities. For example, Section 100a of the German Code of Criminal Procedure sets out the limited number of situations in which telecommunications surveillance will be permitted.[240] Under this Section, communications can only be intercepted "without the knowledge of the persons concerned" if "certain facts give rise to suspicion" that they

[236] R A Miller, *Privacy and Power*, Cambridge, 2017, pg. 350
[237] Article 10(1) Basic Law for the Federal Republic of Germany
[238] D P Kommers, *The Constitutional Jurisprudence of the Federal Republic of Germany*, 2nd Edition, London, 1997, pg. 335
[239] F H Cate & J X Dempsey, *Bulk Collection*, Oxford, 2017, pg. 61
[240] s100a(1) The German Code of Criminal Procedure, StPO

have committed or attempted to commit a "serious criminal offence".[241] In addition to the offence being of a "particular gravity", "other means of establishing the facts or determining the accused's whereabouts" should be "much more difficult or offer no prospect of success".[242] Subsection two lists the crimes amounting to a "serious criminal offence", including acts ranging from "crimes against the peace", to "counterfeiting money", and "crimes against competition".[243] In comparison to the 'offences' originally deemed acceptable for surveillance under the UK Regulation of Investigatory Powers Act, this legislation appears both reasonable and proportionate.[244] Moreover, Section 100b further restricts these orders, providing that they must be applied for by the public prosecution office and ordered by a court, acting in a similar manner to the double lock system utilised by the Investigatory Powers Act in the UK.[245]

The above structure set out by the Code of Criminal Procedure for interception of communications is undoubtedly one of the strictest frameworks for authorising surveillance currently existing in Europe. However, the broad protection offered by the Code, and Article 10 of the Basic Law, has needed judicial interpretation and expansion to ensure that it remains effective in light of modern technological developments. This was illustrated in the 2006 *Data Screening opinion*, in which the German Constitutional Court clamped down on the practice of 'data mining', or *rasterfahndung*.[246] Following the 9/11 terrorist attacks in New York, the German Police collected personal data from over 5.2 million citizens, with the purpose of discovering 'sleeper terrorists'.[247] In regulating this practice, German state laws permitted the access to citizens' data for the purposes of the investigation of past crimes,

[241] Ibid.
[242] Ibid.
[243] Ibid., s100a(2)
[244] See page 47 above.
[245] s100b The German Code of Criminal Procedure, StPO,
[246] Judgement of 4th April 2006, 115 BVerfGE 320, 341–66. P M. Schwartz, *Systematic government access to private-sector data in Germany*, International Data Privacy Law, 2012, Vol.2, No.4, pg. 292
[247] Ibid.

authorised under Section 98a of the Code of Criminal Procedure, and also for preventing criminal activity prior to an offence occurring.[248] The Constitutional Court held that the right to informational self-determination could be limited by acts such as data-screening, but only if it was a proportionate reaction to a "concrete danger", and therefore the latter purpose of the state law was unconstitutional.[249] Furthermore, the Constitutional Court gave effect to the general right of personality, guarded under Articles 2(1) and 1(1) of the Basic Law, stating that it was a "gap filling guarantee" that "is especially required against the background of novel dangers for the development of personality that appear in accompaniment to the progress of science and technology".[250] However, notably, the Constitutional Court did not call this form of surveillance per se disproportionate.[251] Moreover, in defining what they would consider to be a "concrete danger", the Court permitted the continuance of pre-crime investigations, stating that there only had to be a "prognosis of probability" that an offence would occur.[252] This was said to include "factual clues for the preparation of terrorist attacks or the presence in Germany of persons who are preparing terrorist attacks that in the near future will be perpetrated in Germany or elsewhere".[253] Nevertheless, the Court were apt to accompany this allowance with the qualification that "[v]ague clues or bare suppositions are not sufficient".[254]

One further piece of German surveillance legislation not yet mentioned in this analysis is the Act on the Restriction of the Security of Correspondence, Postal, and Telecommunications 1968, also known as the 'Article 10 Act'.[255] This legislation permits the

[248] Ibid.
[249] Judgement of 4th April 2006, 115 BVerfGE 320, 341–66. F H Cate & J X Dempsey, *Bulk Collection,* Oxford, 2017, pg. 68.
[250] Ibid., pg. 64
[251] Judgement of 4th April 2006, 115 BVerfGE 320, 341–66. P M. Schwartz, *Systematic government access to private-sector data in Germany,* International Data Privacy Law, 2012, Vol.2, No.4, pg. 293
[252] Ibid.
[253] Ibid.
[254] Ibid.
[255] Act on the Restriction of the Security of Correspondence, Postal, and Telecommunications 1968

state to collect telecommunications data, and further authorises the procedures of processing this information once obtained, and its subsequent use in criminal proceedings.[256] Although Article 10 of the Basic law protects German citizens' right to privacy of their communications, it can be restricted for particularly important reasons, and by statute, which was provided for by this Act.[257] Under the legislation, if there is individual probable cause to do so, surveillance can be instructed against the data of German citizens, other persons resident in Germany, and any other legal entities.[258] Furthermore, Section 5 permits "strategic surveillance", involving the "filtering, screening and analysis of broad swathes of communications activities in order to identify targets about which there was no previous discrete suspicion".[259] In a similar manner to that proposed by the UK Prime Minister, this Act allows authorities to justify mass preventive surveillance on the premise of searching for the "needle in the haystack".[260] However, this legislation has also been subject to significant legal challenges, most notably the *G10 Decision* in 1999.[261] In finding several parts of the statute unconstitutional, in light of Article 10 of the Basic Law, the Court further stated that the levels of surveillance permitted would lead to "a nervousness in communication, to disturbances in communication, and to behavioural accommodation, in particular to the avoidance of certain content of conversations or terms".[262] Whilst the Court did in part find that the surveillance could have a strong justification, and declared the statute generally "not improper", they found issue with the lack of restrictions on sharing data of those who have

[256] Ibid.
[257] *GFF and Amnesty are challenging strategic mass surveillance*, N Markard, Freiheitsrechte, 6th November 2016, Accessed via https://freiheitsrechte.org/g10/ on 08/09/2018
[258] s3 Act on the Restriction of the Security of Correspondence, Postal, and Telecommunications 1968
[259] R A Miller, *Privacy and Power*, Cambridge, 2017, pg. 356
[260] Ibid.
[261] Judgement of 14th July 1999, 100 BVerfG 313
[262] Ibid., at 381

only committed minor offences, and not simply in serious crimes, as was previously permitted.[263]

Nevertheless, whilst the premise of "German exceptionalism", entrenched in the constitutional protections of the Basic Law, may have survived encroachments made in the late nineties and early 2000's, it is doubtful that such an assessment could be made today. Over the past two years the Bundestag has introduced, in a relatively quiet manner, legislation that provides German authorities with surveillance powers on a par, and perhaps beyond, those of their British counterparts. Some scholars claim that the first signs of this new German approach to surveillance were apparent in the policing of the 2006 FIFA World Cup.[264] Following the tournament, the German authorities were highly criticised by the Commissioners for Data Protection for keeping the personal information of over 250,000 spectators, to be used in background checks for future events.[265]

However, it is arguably the several terrorist attacks in Germany in the past few years that have provided the Government with the necessity, or in the eyes of some the excuse, to enact several laws permitting a greater degree of electronic surveillance. In 2015, the Bundestag passed the "Gesetz zur Einführung einer Speicherfrist und einer Höchstspeicherfrist für Verkehrsdaten", or 'Act Introducing a Storage Obligation and a Maximum Retention Period for Traffic Data'.[266] This legislation, in the same light as the UK's DRIPA, required telecommunications providers to retain their users' data.[267] In October of 2016, the Bundestag then passed the 'Act for Foreign-Foreign Signals Intelligence

[263] P M. Schwartz, *Systematic government access to private-sector data in Germany*, International Data Privacy Law, 2012, Vol.2, No.4, pgs. 292, 293
[264] V Eick, *Lack of Legacy? Shadows of Surveillance after the 2006 FIFA World Cup in Germany,* Urban Studies, 2011
[265] Ibid., pg. 3334
[266] Act Introducing a Storage Obligation and a Maximum Retention Period for Traffic Data 2015
[267] However, the Higher Administrative Court of North Rhine-Westphalia held this law to be invalid and in violation of EU law, therefore its future is currently uncertain. See Oberverwaltungsgericht NRW [Higher Administrative Court of NRW], June 22, 2017, docket no. 13 B 238/17.

Gathering of the Federal Intelligence Service', which amended the previous 'Act on the Federal Intelligence Service'.[268] These amendments, proposed in reaction to the release of the Snowden files, were argued to restrict the powers of the BND, and only permit the surveillance of foreign nationals abroad.[269] Whilst this law limited the surveillance of EU citizens in all cases except those of terrorism, it also stated that it could not be ruled out that the communications of German citizens would be intercepted in its operations, a practice that was previously legally prohibited to the security service.[270] Therefore, in the same way that the UK's Investigatory Powers Act 'restricted' GCHQ by authorising their previously unlawful actions, the legislation passed by the Bundestag allows the BND to 'accidentally' spy on German citizens in a legal manner.

Although the above 2016 legislation may have allowed the authorities greater powers under the veil of restrictions, there was no such subtlety in the changes that followed in 2017. Under the Federal Data Protection Act, passed in June 2017, the "video surveillance of publicly accessible spaces" was legalised in certain circumstances where it was deemed necessary "for public bodies to perform their tasks", "to exercise the right to determine who shall be allowed or denied access", or "to safeguard legitimate interests for specifically defined purposes".[271] This could only operate in "large publicly accessible facilities, such a sports facilities, places of gathering and entertainment, shopping centres and car parks" or "vehicles and large publicly accessible of public rail, ship or bus transport".[272] Even though this definition could be deemed to be fairly wide scoping in permitting nearly all possible

[268] Act for Foreign-Foreign Signals Intelligence Gathering of the Federal Intelligence Service 2016
[269] *German parliament approves controversial espionage law*, J Nasr, Reuters, 21st October 2016, Accessed via https://www.reuters.com/article/us-germany-spying/german-parliament-approves-controversial-espionage-law-idUSKCN12L1ER on 08/09/2018
[270] Ibid.
[271] Act to Adapt Data Protection Law to Regulation (EU) 2016/679 and to Implement Directive (EU) 2016/680 (DSApUG-EU) of 30 June 2017, s4(1)
[272] Ibid.

public spaces, it was clearly in reaction to the recent attacks occurring in crowded German city areas, and on public transport.

In other European states, most notably the United Kingdom, this increase in video surveillance would be a fairly uncontroversial proposition, yet due to Germany's past distrust for Government monitoring, it raised a considerable amount of apprehension amongst civil liberties advocates and the German public alike. Nevertheless, what was far more concerning was the Act's stipulation that the protection of "the lives, health and freedom of persons present shall be regarded as a very important interest".[273] Through providing these security concerns with the status of a "very important interest", this legislation effectively diminished the previously inviolable right to privacy, opening the floodgates for future encroachments on this foundational liberty of Germany. Although the increase in video cameras in public places may cause privacy activists great unease, it is this shift in position on what was previously an untouchable right that signals the most significant change in the German approach to surveillance, and the death of the previous ideals of Germany's exceptionalism.

As discussed in the first chapter, the German Bundestag then went on to amend the Code of Criminal Procedure, permitting the installation of "state trojans" onto citizens' electronic devices to monitor their communications.[274] Through the "Act to Make Criminal Proceedings More Effective and Practicable", the Bundestag controversially legalised the practice of gaining information from a technological device without the suspects consent or knowledge.[275] This form of "source telecommunication surveillance" allows the German authorities to access information on mobile devices before it is encrypted, thereby providing a wealth of communications data without having to encounter the issues of key disclosure

[273] Ibid.
[274] See page 18 above.
[275] Article 3(9) Act to Make Criminal Proceedings More Effective and Practicable 2017

discussed in the first chapter.[276] Far away from the previous idealism of 'German exceptionalism', this power permits the German authorities to invade the privacy of their citizens to the same degree as their British and American counterparts.

c) Pre Crime Surveillance

However, when considering the conflict between surveillance and the presumption of innocence, it is the issue of pre-crime policing, apparent in both Germany and the United Kingdom, which raises the potential for these arguments to be made. As described by Zedner, whilst in a post-crime society there are offenders, victims, investigation, and punishment; pre-crime investigation "shifts the temporal perspective to anticipate and forestall that which has not yet occurred and may never do so", where there is risk, uncertainty, and surveillance.[277] Relying on computer software and statistics rather than investigations and evidence, this form of preventive policing seeks to predict what type of crime will occur, where and when it will happen, and how it can be stopped.[278] As the role of policing in society shifts to crime control and deterrence, intelligence gathering technology has become increasingly important, to the point where now nearly every person is subject to criminal investigation through surveillance practices.[279] In order for the preventive pre-crime model to work, everyone must be considered to be a potential offender, regardless of their actual innocence.[280]

[276] *German federal police use Trojan virus to evade phone encryption*, C Burack, DW, 27th January 2018, Accessed via https://www.dw.com/en/german-federal-police-use-trojan-virus-to-evade-phone-encryption/a-42328466 on 09/09/2018
[277] O Olugasa, *Rethinking Pre-Crime Surveillance versus Privacy in an Increasingly Insecure World: Imperative Expediency,* Journal of Law, Policy and Globalisation, 2017, pg. 188
[278] J Vlahos, *The Department of Pre-Crime,* Scientific American, 2012, pg. 64
[279] A Galetta, *The changing nature of the presumption of innocence in today's surveillance societies: rewrite human rights or regulate the use of surveillance technologies?,* European Journal of Law and Technology, 2013, pg. 3
[280] Ibid.

This understandably appears on its face to be a dystopian threat, present only in science fiction novels or feature films, such as *Minority Report*.[281] However, preventive policing is an undeniable reality. As discussed above, the "thematic warrants" authorised under the Investigatory Powers Act 2016 allow UK authorities to intercept the communications and interfere with the equipment of large groups of citizens at a time, where it is necessary for "preventing" crime.[282] It has also been reported that the British police have been harnessing statistical evidence to try and predict a range of crimes, which when combined with the powers authorised under the 2016 Act, permits the authorities to access the data of individuals who are in no way connected to a criminal offence, other than being present in a certain area.[283] On the other hand in Germany, the aforementioned *Data Screening* decision restricted the use of surveillance in a widespread preventive nature, stating that there had to be a "concrete danger" that a serious crime would occur.[284] Nonetheless, this "concrete danger" only had to be based a "prognosis of probability" that the harm would occur.[285] Furthermore, in the *Preventive Telecommunications Surveillance* opinion of the previous year, the Constitutional Court explicitly authorised this practice in situations where "there was an especially high ranking endangered legal interest and a designated situation with concrete stopping points and a connection through direct references to the future carrying out of a criminal offence".[286] The German authorities have also deployed statistical policing to prevent offences, known as the "Pre-crime observation

[281] *Why Minority Report was spot on*, C Arthur, The Guardian, 16th June 2010, Accessed via https://www.theguardian.com/technology/2010/jun/16/minority-report-technology-comes-true on 22/09/2018
[282] s101, 108(3(b)) Investigatory Powers Act 2016
[283] *How technology is allowing police to predict where and when crime will happen*, L Dearden, The Independent, 7th October 2017, Accessed via https://www.independent.co.uk/news/uk/home-news/police-big-data-technology-predict-crime-hotspot-mapping-rusi-report-research-minority-report-a7963706.html on 22/09/2018
[284] P M. Schwartz, International Data Privacy Law, 2012, pg. 223
[285] Ibid.
[286] 113 BVerfGE 348, 392 (2005) (Preventive Telecommunications Surveillance). P M. Schwartz, *Systematic government access to private-sector data in Germany*, International Data Privacy Law, 2012, pg. 225

system".[287] Whilst this is only being used on a trial basis, it again signals a move towards a pre-crime and prevention based policing system, utilising statistics and surveillance to render the whole society as untrustworthy.

Generally, it can be claimed that there are two types of preventive policing employed by law enforcement agencies around the world.[288] The first use is in situations where people who have already committed one offence, or have been suspected of a previous crime, are monitored due to their apparent likelihood for criminal activity.[289] Often this can be seen in the form of databases collecting data on those who have been previously arrested or convicted of a crime, which is then used to justify their later surveillance.[290] It can also lead to the active intervention of the authorities in the lives of previous offenders. For example, police in Scotland have utilised databases of those suspected of domestic abuse, visiting and thus deterring these individuals around the time of events such as football matches, where statistical data shows that crime is more likely to occur.[291] In London the Metropolitan Police use a "Gangs Matrix", which consists of a list of potential gang members ranked on their likelihood to commit crime.[292] This inventory is compiled through various sources, including the surveillance of social media and online activity, from which the Police inform their decisions on who to exercise stop and search powers on.[293] Although such policing can serve an undeniable social good, it also has the potential to treat individuals who have never actually committed an offence as criminals, and thus denigrate their image in society. This

[287] *Tracking patterns: how software claims to stop crime by analysing a burglar's behaviour*, V Betz, DW, 11th December 2014, Accessed via https://www.dw.com/en/tracking-patterns-how-software-claims-to-stop-crime-by-analyzing-a-burglars-behavior/a-18109666 on 22/09/2018
[288] O Olugasa, *Rethinking Pre-Crime Surveillance versus Privacy in an Increasingly Insecure World: Imperative Expediency*, Journal of Law, Policy and Globalisation, 2017, pg. 187
[289] Ibid.
[290] See *S. and Marper v. The United Kingdom*, Application no. 36562/04, 2008
[291] K Hadjimatheou, *Surveillance: Ethical Issues, Legal Limitations, and Efficiency,* SURVEILLE, 2013, pg. 13
[292] Amnesty International, *Trapped in the Matrix: Secrecy, stigma, and bias in the Met's Gangs Database,* May 2018, pg. 6
[293] Ibid., pgs. 6, 7

was indeed illustrated by the use of the "Gangs Matrix", as Amnesty International found that over forty percent of all those on the list had "no record of charges or police intelligence linking them to violence in the past two years".[294]

Furthermore, in attempting to identify previous and potential offenders, authorities in the United Kingdom have employed modern technology to determine whether a crime will take place.[295] For example, at the 2017 Champions League final in Cardiff, the UK authorities used facial scanning technology to try and pick out people whose faces matched those of custody photos.[296] There were 2470 potential matches identified by the system, however 92% (2297) were incorrect.[297] Despite no action being taken by the authorities on that day, this illustrates the significant dangers posed by using preventive policing, as not only is it highly speculative, but it also could lead to the wrongful criminalisation and arrest of innocent citizens.

The second type of preventive policing does not act with the same degree of specificity, and instead interferes with the lives of every citizen, acting on the premise that if the authorities broadly survey a large group of people, it becomes more likely that they will be able to prevent crime. Referred to as "untargeted surveillance", this practice involves the interception of communications of all individuals who are in a certain location or are engaged in a specific activity.[298] In addition to the sweeping access to data, this form of prevention also encompasses the use of statistical evidence to predict exactly when and where a crime may occur. This has been extensively used in Richmond, Virginia, where the police use the information obtained from previous offences to offer a probability analysis of specific areas

[294] Ibid., pg. 7
[295] *2,000 wrongly matched with possible criminals at Champions League*, BBC News, 4th May 2018, Accessed via https://www.bbc.co.uk/news/uk-wales-south-west-wales-44007872 on 22/09/2018
[296] Ibid.
[297] Ibid.
[298] K Hadjimatheou, *The Relative Moral Risks of Untargeted and Targeted Surveillance,* Ethic Theory Moral Practice, 2014, pg. 187

of the city where a crime is likely to occur.[299] Even though this may on occasion provide the authorities with the opportunity to prevent a crime from occurring, it also means that innocent people may have their personal lives interfered with solely due to their connections, social status, or location.

iii) Challenging Surveillance under ECtHR and other International Bodies

As is apparent from the challenges to surveillance in the domestic jurisdictions covered, it has been an almost universal approach to contest the legitimacy of this practice on privacy grounds. This is undoubtedly the most obvious restriction on the expansion of state monitoring, and it has been successful before both domestic constitutional courts and international human rights bodies.[300] Furthermore the obligation to regard the privacy rights of citizens when creating legislation on interception of communications has become a common standard around the world, which is reflected in the aforementioned laws of the United Kingdom and Germany on this matter.[301] However, it could be argued that whilst focusing on the right to privacy may be the easiest way to protect citizens against the harms of surveillance, by refusing to look to the other human rights available, civil liberties advocates are failing to properly use all of the tools available to them.

Nevertheless, when examining the case law, treaties, and publications of the international human rights bodies, it becomes understandable why such a privacy-centric approach is taken. For example, the work of the UN Human Rights Committee has enforced a strong tradition of condemning any prospective surveillance of citizens on privacy grounds.[302] This is evident from General Comment 16 on the Right to Privacy, which astutely

[299] *Richmond, Virginia, Police Department Helps Lower Crime Rates with Crime Prediction Software*, C Harris, Government Technology, 21st December 2008, Accessed via http://www.govtech.com/public-safety/Richmond-Virginia-Police-Department-Helps-Lower.html on 25/10/2018
[300] See for example *Szabó and Vissy v. Hungary,* Application no. 37138/14, 2016
[301] See for example s2 Investigatory Powers Act 2016
[302] F H Cate & J X Dempsey, *Bulk Collection,* Oxford, 2017, pg. 359

states that "[s]urveillance, whether electronic or otherwise, interceptions of telephonic, telegraphic and other forms of communication, wire-tapping and recording of conversations should be prohibited".[303] A similar line has followed from the work of the UN Special Rapporteurs, including those covering rights such as expression and opinion, who have recently highlighted and encouraged the respect of the use of encryption technologies, which create "a zone of privacy to protect opinion and belief".[304] However the UN, and indeed other international bodies, have overtime become significantly more tolerant to the idea of Government monitoring. Whilst the aforementioned General Comment 16 called for a prohibition of all surveillance, thirty years later the "Draft Legal Instrument on Government-led Surveillance and Privacy" instead moves to broadly facilitate this practice with vague restrictions mirroring those seen in the domestic legislation discussed above.[305] This is perhaps simply indicative of both the current institutional position on surveillance, and the move of international human rights bodies to pander to states in order to ensure interest and engagement with their processes.

Yet whilst these bodies may be taking a softer approach to Government interference, this has not prevented international courts from moving to criticise and declare violations in cases before them on this subject. For example, the Inter-American Court of Human Rights has taken a strong position on this, as was seen in the case of *Echer et al v. Brazil*, where they held that "the fluidity of information places the individual's right to privacy at greater risk owing to the new technological tools and their increased use", and thus "the State must increase its commitment to adapt the traditional forms of protecting the right to privacy to

[303] CCPR General Comment No. 16: Article 17 (Right to Privacy), UN Human Rights Committee, 8 April 1988, at [8]
[304] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, D Kaye, UN Human Rights Council, 22 May 2015, A/HRC/29/32, at 12
[305] Working Draft Legal Instrument on Government-led Surveillance and Privacy, Version 0.7, February 28 2018, Accessed via https://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2018AnnualReportAppendix7.pdf on 15/09/18

current times".[306] Such a position has also been shared by the ECtHR, who since their inception have held that even the "mere existence" of any Government surveillance would automatically constitute an interference with the Convention.[307] The Court's cornerstone cases on this area involved the other two jurisdictional comparators of this analysis, Germany and the United Kingdom. In the 1978 case of *Klass v. Germany*, the Court held that any surveillance measures "would result in an interference by a public authority with the exercise of that individual's right to respect for his private and family life", and that the legislation itself would mean that those who it applied to automatically had their rights interfered with.[308] Although a violation was not found in this case, it remains a crucial piece of jurisprudence in ensuring that Article 8 can always be relied upon when challenging surveillance.[309] In the later case of *Malone v. the United Kingdom,* the applicant claimed that in convicting him for the possession of stolen goods, the UK authorities had intercepted his communications, and thus, violated Article 8 of the Convention.[310] Following the precedent set in *Klass,* it was held to be a clear interference with the Convention, however unlike the previous case, the Court also went on to find a violation, due to the UK legislation not meeting the foreseeability requirements of the "in accordance with the law" criterion.[311]

Since these decisions, the Court has maintained a firm line on surveillance, and in recent years have moved to specify exactly what practices they will find to be in violation of privacy rights. In *Roman Zakharov v. Russia,* the Court took a significant step against mass surveillance practices, finding a violation due to the Russian law's authorisation procedures not ensuring that measures were imposed only when "necessary in democratic society".[312]

[306] *Case of Escher et al. v. Brazil*, Judgment of July 6 2009, IACtHR, at 115
[307] F H Cate & J X Dempsey, *Bulk Collection,* Oxford, 2017, pg. 365
[308] *Klass and Others v. Germany,* Application no. 5029/71, 1978, § 41
[309] Ibid., § 60
[310] *Malone v. The United Kingdom*, Application no. 8691/79, 1984, §§ 16, 17
[311] Ibid., §§ 63, 80
[312] *Roman Zakharov v. Russia,* Application no. 47143/06, 2015, § 302

This position was furthered in *Szabó and Vissy v. Hungary*, where the Court recognised the technological changes since *Klass,* stating that *"*the potential interferences with email, mobile phone and Internet services as well as those of mass surveillance attract the Convention protection of private life even more acutely".[313] Due to the "potential of cutting-edge surveillance technologies to invade citizens' privacy", the "necessary in a democratic society" criterion had to instead be interpreted as requiring "strict necessity".[314] This requirement entailed that the surveillance had to be strictly necessary "for the safeguarding of the democratic institutions" and "for the obtaining of vital intelligence in an individual operation".[315] The lack of proper judicial authorisation for surveillance in Hungary led the Court to find that "the scope of the measures could include virtually anyone", thus amounting to a violation of Article 8.[316]

The most recent decision by the ECtHR concerning Article 8 and surveillance is that of *Big Brother Watch and Others v. the United Kingdom.*[317] This case concerned a legal challenge to the aforementioned Regulation of Investigatory Powers Act 2000, on the basis that the interception warrants lacked proper judicial safeguards, and that the practice of sharing intelligence information gained through surveillance with other nations violated Article 8 of the Convention.[318] In their decision, the Court held that the "lack of oversight" on the interception of communications" and the "absence of any real safeguards" for the "selection of related communications data for examination" meant that the Act failed to meet the "quality of the law" requirement, and was thus incapable of restricting the interference with Article 8 to solely what is "necessary in a democratic society", building upon the 'strict

[313] *Szabó and Vissy v. Hungary,* Application no. 37138/14, 2016, § 53
[314] Ibid., § 73
[315] Ibid.
[316] Ibid., § 89
[317] *Big Brother Watch and Others v. The United Kingdom,* Application no. 58170/13, 2018
[318] Ibid., § 269

necessity' criterion of *Szabo and Vissy.*[319] This decision was hailed by many as an important victory in stifling Government surveillance in the United Kingdom, with Amnesty International stating that "[t]oday's ruling represents a significant step forward in the protection of privacy and freedom of expression worldwide".[320]

However, such celebration is arguably premature. As noted by Jim Killock, the executive director of Open Rights Group, since the case started "the UK has actually increased its powers to indiscriminately survey our communications whether or not we are suspected of any criminal activity", through the previously mentioned Investigatory Powers Act 2016.[321] What is perhaps more troubling is, as was previously discussed, the 2016 Act has greater, yet ineffective, safeguards through the "double lock" system which would potentially meet the ECtHR's standard, and thus not amount to a violation of Article 8.[322] Therefore, future legal challenges under this right may prove to be without adequate merit, and it becomes necessary to seek new approaches to confront these investigative practices, such as through the use of the right to a fair trial.

iv) The Presumption of Innocence

In a similar manner to the privilege against self-incrimination, the presumption of innocence is a legal principle entrenched in hundreds of years of history. Its earliest use is arguably found in the 6th Century Roman law writings of the Digest of Justinian, where it was stated that it was "preferable that the crime of a guilty man should go unpunished than an innocent man be condemned".[323] Harkening to a renowned moral principle, this later became entrenched in domestic jurisprudence around the world, forming criminal law procedures that

[319] Ibid., §§ 387, 388
[320] *GCHQ data collection regime violated human rights, court rules*, O Bowcott, The Guardian, 13th September 2018, Accessed via https://www.theguardian.com/uk-news/2018/sep/13/gchq-data-collection-violated-human-rights-strasbourg-court-rules on 15/09/18
[321] Ibid.
[322] See page 49 above.
[323] A Stumer, *The Presumption of Innocence: Evidential and Human Rights Perspectives*, Oxford, 2010, pg. 2

sought to ensure that no one innocent was convicted. The 13th Century 'Laws and Customs of England" provided a formulation more similar to what is seen in statute books today, stating that "it is presumed that every man is good until the contrary is proved".[324] William Blackstone's primary legal formulation in his 18th Century work also followed in this ideal, where he claimed that "it is better that ten guilty persons escape than that one innocent suffer".[325]

However the presumption, often referred to by its Latin origins of *in dubio pro reo*, only became an assured part of the British common law in the 1935 case of *Woolmington v. DPP*, which concerned the alleged accidental shooting of a woman by her husband.[326] In his infamous 'Golden thread' speech, Viscount Sankey stated that "[t]hroughout the web of the English Criminal Law one golden thread is always to be seen that it is the duty of the prosecution to prove the prisoner's guilt" and that "[n]o matter what the charge or where the trial, the principle that the prosecution must prove the guilt of the prisoner is part of the common law of England and no attempt to whittle it down can be entertained".[327] In Germany, the presumption of innocence, known as *unschuldsvermutung*, has a basis in the rule of law principles of the Basic Law, found under Article 20(3) and 28(1).[328] Nevertheless, the presumption only exists truly within the German Law, and has evolved in British Law, due to both countries' incorporation of the ECHR.[329]

The presumption of innocence appears in the Convention under Article 6(2), where it states that "[e]veryone charged with a criminal offence shall be presumed innocent until

[324] Ibid.
[325] Ibid., pg. 3
[326] *Woolmington v DPP*, [1935] UKHL 1
[327] Ibid.
[328] Article 20(3), 28(1), Basic Law for the Federal Republic of Germany
[329] T Weigend, *Assuming that the Defendant Is Not Guilty: The Presumption of Innocence in the German System of Criminal Justice*, Criminal Law and Philosophy, 2014, pg. 286

proved guilty according to law".[330] As put forward by Andrew Stumer, there are three current judicial formulations of the presumption of innocence in the jurisprudence of the ECtHR; "a principle prohibiting official decisions reflecting guilt in the absence of a prior judicial determination, a principle placing the burden of proof on the prosecution and giving the defendant the benefit of any doubt, and a principle requiring presumptions of fact or law to be confined within reasonable limits".[331] The first holding prevents judicial decisions, or public officials, from implying that an individual is guilty of a crime following their acquittal before a court. This was shown in *Minelli v. Switzerland,* where an acquitted individual was forced to pay the majority of the case costs, suggesting they were guilty, even though such a judicial determination was not found.[332] The finding of a violation in this regard serves to protect the reputation of the individual, and to counter the risk that the guarantees of Article 6 become "theoretical and illusory".[333] Furthermore, as held in *Allenet de Ribemont v. France*, this principle also extends to the statements of public officials prior to a trial.[334] This case concerned remarks made by a senior police officer, where he claimed that the applicant was the instigator of a murder.[335] The Court held that the presumption of innocence would be violated if a judicial decision, or a statement of other public officials, reflected an opinion that a "person charged with a criminal offence…is guilty before he has been proved guilty according to law".[336] This significantly expanded the presumption beyond the context of a trial, and to further encompass the actions of individuals other than the judiciary.

The second formulation restates the general legal principle of the "burden of proof" remaining on the prosecution. The case law of the Court has ensured this, clearly stating that

[330] Article 6(2) ECHR
[331] A Stumer, Oxford, 2010, pgs. 89, 90
[332] *Minelli v. Switzerland,* Application no. 8660/79, 1983, § 13
[333] Harris et al, *Law of the European Convention on Human Rights,* 3rd Edition, Oxford, 2009, pg. 464
[334] *Allenet de Ribemont v. France,* Application no. 15175/89, 1995
[335] Ibid., § 20
[336] Ibid., § 35

"the presumption of innocence will be infringed where the burden of proof is shifted from the prosecution to the defence".[337] However, as seen in the case of *Lingens v. Austria*, this will not apply for all cases, for example in the circumstances of the special defence of truth in libel proceedings.[338] The third and final interpretation provided by Strumer concerns presumptions of fact or law being "confined within reasonable limits", again striving to prevent the reversal of the burden of proof. This was most prominently discussed by the Court in the case of *Salabiaku v. France*, where the applicant was caught at customs collecting a package of 10kg of cannabis, and was convicted of importing prohibited goods.[339] The applicant claimed that he was expecting the parcel to "contain samples of African food", however the domestic court held that he would be presumed to be the owner of the previous package unless he could prove a "specific event of force majeure exculpating him".[340] In considering whether Article 6(2) had been violated, the ECtHR stated that the Convention required states to confine presumptions of fact or of law "within the reasonable limits which take into account the importance of what is at stake and maintain the rights of the defence".[341] In the case of Mr Salabiaku, this had been ensured by the domestic French court through considering all the facts, and therefore no violation was found.[342]

The Strasbourg Court's approach to the presumption of innocence and Article 6(2) thus covers a wide range of cases, and provides individuals with a comprehensive criminal procedure right. This could be argued to assist individuals for which unlawful or disproportionate surveillance has led to their conviction. First of all, it can be argued that the practice of surveillance in general will have a significant impact on the accused in criminal

[337] *Telfner v. Austria*, Application no. 33501/96, 2001, § 15
[338] *Lingens v. Austria*, Application no. 8803/79, 1982
[339] *Salabiaku v. France*, Application no. 10519/83, 1988, §§ 9, 10
[340] Ibid., §§ 9, 14
[341] Ibid., § 28
[342] Ibid., § 29

proceedings, due to the nature and gravity of the information that will be held against them.[343] As previously discussed, the presumption of innocence places a burden on the prosecution to prove the suspect's guilt, and provides the accused with the benefit of the doubt before this is achieved.[344] However, when surveillance has been carried out by the authorities both during the investigation period, and potentially before through mass monitoring, the burden of proof will be de facto overturned at the trial stage.[345] As the evidence available to the prosecution will be vast, and often not known to the individual, the "cross-examination stage of the trial focuses on the surveillance evidence and on evidences that the defendant is able to provide in order to prove himself innocent".[346] The final decision of the Court, instead of turning on the prosecution's ability to prove the defendant guilty, will be reliant on the capability of the accused from the outset to rebut the evidence held against them.[347] The European Court of Human Rights have repeatedly held that Article 6(2) requires the burden of proof to be placed and remain on the "prosecution", and that at all stages "any doubt should benefit the accused".[348] The collection of data from individuals on such a large scale by states would thus undermine the presumption's guarantees in a trial setting, and potentially be held to violate the Convention. However, the jurisprudence of the Court is not without limitation, as it only applies to those who have been subject to a "criminal charge", and not those simply under suspicion.[349] As surveillance almost exclusively occurs prior to a charge being issued, and is increasingly used against the whole population at any point, it is

[343] D Wright & R Kreissl, *Surveillance in Europe*, London, 2015, pg. 287
[344] M Mendola, *One Step Further in the 'Surveillance Society': The Case of Predictive Policing,* Tech and Law Center, 2016, pg. 11
[345] J Milas et al, *Unwitting subjects of surveillance and the presumption of innocence,* Computer Law & Security Review 30, 2014, pg.425
[346] A Galetta, European Journal of Law and Technology, 2013, pg. 4
[347] D Wright & R Kreissl, *Surveillance in Europe*, London, 2015, pg.
[348] See *Barberà, Messegué and Jabardo v. Spain,* Application no. 10590/83, 1988, § 77
[349] Harris et al, *Law of the European Convention on Human Rights,* 3rd Edition, Oxford, 2009, pg. 460

thus necessary to analyse further theoretical interpretations of the presumption in order to determine whether government interceptions interfere with it.

Outside of the strict confines of the ECtHR's jurisprudence, legal theorists have taken wider interpretations of the presumption of innocence. For example according to Weigend, "the very aim of the presumption of innocence is to protect the suspect from overbearing situations as a consequence of state actions", and therefore "prohibits state agents from taking action that necessarily presupposes that the suspect is in fact guilty".[350] This could apply prior to the provision of a criminal charge, and extend to the investigation stage of the proceedings.[351] This is a position not shared by many common law jurisdictions, such as the United States, who in the Supreme Court case of *Bell v. Wolfish* held that the presumption could only properly apply in the context of a criminal trial.[352] However, if following Weigend's interpretation, the presumption could stretch to the imposition of surveillance on an individual or group of persons prior to a trial, where they could argue that through its use they were being presumed guilty.

This is undoubtedly a large step beyond what is currently accepted by Courts around the world, however in terms of the arguments made by various legal writers, it is relevantly tame. For example, many scholars argue that the presumption should be held to apply in the pre-adjudicative context, prior to a charge being issued, where suspects and persons of interest should be treated and regarded as "if their guilt has not yet been authoritatively established".[353] Others such as Hamish Stewart go one step further, stating that we should see the presumption of innocence in even a pre-suspicion context, which could encompass the

[350] F de Jong & L van Lent, *The Presumption of Innocence as a Counterfactual Principle*, Utrecht Law Review, 2016, pg. 35
[351] Ibid., pg. 38
[352] *Bell v. Wolfish*, 441 U.S. 583 (1979)
[353] R L Lippke, *Taming the Presumption of Innocence*, Oxford Scholarship Online, 2016, pg. 7

use of mass surveillance.[354] Instead of a right confined to the context of a trial, Stewart views the presumption in terms of an "innate moral right to be presumed innocent", any infringement of which should therefore have to be justified.[355]

In analysing the theoretical interpretations of the presumption of innocence, and indeed any criminal procedure right, it is crucial to view it from the position of what wrong is trying to be prevented. One such evil, which was discussed in the previous chapter in reference to the purposes of the privilege against self-incrimination, is wrongful criminalisation. As argued by Hadjimatheou, a failure to adhere to the presumption of innocence prior to charge could also result in the wrongful criminalisation of innocent citizens.[356] This becomes particularly threatening when it comes to the issue of stigmatisation, as if certain groups are targeted for investigation by the authorities without the protection of the presumption of innocence at this early stage, their rights can be significantly affected. As will be discussed below, the potential for these wrongs to have an effect is of particular relevance to the issue of pre-crime surveillance, and even has recognition in the jurisprudence of the ECtHR.[357]

However, there is one final interpretation of the presumption of innocence, related to the aforementioned harm of stigmatisation, known as the 'principle of civility' or the 'right to be treated as trustworthy'.[358] As argued by Nance, "the principle of civility imposes a duty on all people to treat each other as if they have been and are acting in accordance with their important social obligations, included but not limited to respect for the criminal law".[359] Through failing to treat people as if they are trustworthy, we instead treat them as if they are

[354] Ibid.
[355] Ibid., pgs. 7, 9
[356] K Hadjimatheou, *Surveillance Technologies, Wrongful Criminalisation, and the Presumption of Innocence*, Springer, 2017, pg. 42
[357] See page 76 below.
[358] K Hadjimatheou, Springer, 2017, pg. 43
[359] Ibid.

guilty of a social, moral, or legal indiscretion, and thus lower their status in the community. This falls in line with Anthony Duff's 'principle of civic trust', which imposes a "duty to treat people as if they will continue to act in accordance with their important obligations".[360] In addition to protecting individuals prior to their charging by the police, Duff's principle also mirrors the recognised standard provided by the ECtHR, as in the absence of a guilty verdict, the Convention places an onus on public authorities to resist from treating or presenting individuals as if they have committed an offence.[361] In regards to the presumption's conflict with the use of surveillance technologies, it is this restriction on untrustworthiness that is of particular relevance. Through imposing surveillance on civilians, the authorities automatically mark them as untrustworthy individuals, and thus, as guilty and not innocent.

Nevertheless, it has to be conceded that in a law abiding society the police should have the power, authority, and resources to investigate crimes, arrest suspects, and secure evidence.[362] As much as civil liberties campaigners may wish for restrictions on the advanced technologies that can be utilised against such suspects, it is difficult to argue with the fact that upon the commission of a criminal offence, the authorities should have the power to use the resources available to them to fulfil their role in the community, albeit with the appropriate regulations. However, as was briefly discussed above in relation to the current surveillance practices of the United Kingdom and Germany, states have in recent years moved beyond the traditional modes of investigating crimes, and now instead attempt to prevent offences prior to their commission. Whilst there is certainly an argument to be made that Article 6 ECHR is

[360] Ibid.
[361] *Allenet de Ribemont v. France*, Application no. 15175/89, 1995, § 35
[362] R L Lippke, *Taming the Presumption of Innocence*, Oxford Scholarship Online, 2016, pg. 11

interfered with in all interceptions of communications, it is within this use of pre-crime surveillance that this chapter will argue that the presumption of innocence is truly violated.

v) Conflict between Preventive Surveillance and the Presumption

First of all, it can be argued that the use of preventive surveillance has the potential to infringe upon the presumption in regards to the "right not to be stigmatised as criminally suspicious".[363] This is particularly relevant in situations of targeted preventive surveillance, where individuals who have previously been convicted, arrested, or even just suspected of a previous offence are subject to monitoring from the state. In the United Kingdom, this saw the creation of databases of 'pre-suspects', where the authorities held information on individuals who they deemed likely to become suspects in future investigations.[364] This was highlighted in the case of *S & Marper*, where the applicants claimed that the UK's practice of retaining fingerprints and DNA samples, even in situations where the individual was not prosecuted or was acquitted, was in violation of Articles 8 and 14 of the Convention.[365] Although Article 6(2) was not claimed by the applicants, the ECtHR recognised that the practice of retaining this data had a potentially stigmatising effect, which could interfere with the presumption of innocence. In their decision the Court stated that "of particular concern in the present context is the risk of stigmatisation, stemming from the fact that persons in the position of the applicants, who have not been convicted of any offence and are entitled to the presumption of innocence, are treated in the same way as convicted persons".[366] Furthermore, although they conceded that this action could not be directly equated with the aforementioned violations when suspicions are raised following an acquittal, the "perception that they are not being treated as innocent is heightened by the fact that their data are retained indefinitely in

[363] K Hadjimatheou, SURVEILLE, 2013, pg. 5
[364] Ibid., pg. 5
[365] *S. and Marper v. The United Kingdom*, Application no. 30562/04, 2008, § 3
[366] Ibid., § 122

the same way as the data of convicted persons, while the data of those who have never been suspected of an offence are required to be destroyed".[367] Whilst this case was not directly to do with the use of preventive surveillance, the recognition of the conflict of the presumption of innocence and stigmatisation has been argued to illustrate a "stepping stone towards the recognition of the "right of the surveyed to be presumed innocent" until proven guilty".[368]

However, the stigmatising effect caused by surveillance is not limited to the retention of data on previous subjects, and can also arise in the context of pre-crime policing. In this regard, the conflict with the presumption is not strictly caused by surveillance and collection of data, but instead is due to the later intervention by the police following this monitoring. As later interactions with the authorities will be based on computer programming, rather than concrete evidence, innocent civilians will be affected through circumstances out of their control. For example, in the aforementioned *Data Mining* opinion of the German Constitutional Court, the law in question was partly struck down due to the stigmatising effect that it had on those civilians singled out for investigation, as it unfairly associated them with being connected to terrorism.[369] In these actions, the suspicions held by the police through the use of this technology are no longer based on solely criminal behaviour, but instead rest largely on "marginal behaviour and lifestyles".[370] As described by David Lyon, this can lead to a form of 'social sorting', which can consequentially have a significant effect on a person's inclusion into society.[371] Furthermore, if the data is based upon already flawed arrest statistics, those from minority backgrounds will often face far more interaction with the authorities in the form of arrests and surveillance, simply due to their race, religion, or social

[367] Ibid.
[368] D Wright & R Kreissl, *Surveillance in Europe*, London, 2015, pg. 292
[369] K Hadjimatheou, SURVEILLE, 2013, pg. 5. Judgement of 4th April 2006, 115 BVerfGE 320, 341–66.
[370] J Milas et al, Computer Law & Security Review 30, 2014, pg. 419
[371] K D Haggerty et al, *Theorizing surveillance in crime control*, Sage, 2011, pg. 233

standing.[372] Although this suspicion may be backed by statistical evidence of a higher propensity to commit crime, and thus not entirely wrongfully criminalising, the risk that it stigmatises a whole community with the image of being guilty will undoubtedly interfere with this aspect of the presumption of innocence.[373] As underlined by Dahl and Saetnan, the ultimate consequence of surveillance creates forms of differentiation between "we, the normal, trusted citizens" and "they, the others, the non-trustworthy", so undermining the basic pillars of democracy".[374]

Instead, as has been held by the ECtHR, in order to comply with the presumption, policing should be based upon "reasonable suspicion". This was described in the case of *Ilgar Mammadov v. Azerbaijan*, where the Court stated that "the requirement that the suspicion must be based on reasonable grounds forms an essential part of the safeguard against arbitrary arrest and detention. The fact that a suspicion is held in good faith is insufficient. The words 'reasonable suspicion' mean the existence of facts or information which would satisfy an objective observer that the person concerned may have committed the offence. What may be regarded as 'reasonable' will depend upon all the circumstances".[375]Although a certain behaviour may be believed by the police to lead or be related to criminal activity this does not mean that the employment of surveillance or pre-crime policing will be deemed justifiable.[376] There must be reasonable suspicion.

However, as argued by Hadjimatheou, "to claim that treating people as suspicious on the basis of this kind of behaviour always violates the right not to be stigmatised would restrict the range of cases in which stigmatising surveillance is justified too much to be

[372] Ibid., pg. 233
[373] K Hadjimatheou, Springer, 2017, pg. 46
[374] A Galetta, European Journal of Law and Technology, 2013, pg. 4
[375] *Ilgar Mammadov v. Azerbaijan*, Application no. 15172/13, 2014, § 88
[376] K Hadjimatheou, SURVEILLE, 2013, pg. 12

coherent with a range of common and accepted police practices".[377] The impact that the success of these arguments would have on the standard investigations pursued by domestic authorities would be of such a scale that no judicial body would be likely to uphold them. Furthermore, the argument that surveillance violates the presumption of innocence through its stigmatising effect does not serve to challenge all forms of goverment monitoring. As previously discussed, in recent years states have expanded their communications interceptions to cover not only those who they believe may be involved in criminal activities, but the entire population. Through the use of this "untargeted surveilance", everyone in the country, or at least those with access to an electronic communications device, will be treated equally, and thus no one in particular will be stigmatised.[378] Nevertheless, this does not mean that this practice does not violate criminal procedure laws. Instead, this interferes with the so-called "right to be trusted".[379]

In the use of mass untargeted surveillance, the authorities operate with the logic that every citizen could potentially be involved in criminal activity, and thus everyone is a suspect.[380] It treats innocent people as though they are untrustworthy, even though they have never shown any signs of wrongdoing.[381] This in turn creates what Milas describes as a "culture of suspicion", which "affects mutual trust, social inclusion, and causes a "chilling effect" on criminal procedure rights.[382] Citizens will be presumed guilty until the evidence collected from their communications proves otherwise, allowing the authorities to act without individualised suspicion, thus subverting the presumption of innocence.[383] This amounts to

[377] Ibid.
[378] K Hadjimatheou, Ethic Theory Moral Practice, 2014, pg. 189
[379] K Hadjimatheou, SURVEILLE, 2013, pg. 16
[380] J Milas et al, Computer Law & Security Review 30, 2014, pg. 420
[381] K Hadjimatheou, Ethic Theory Moral Practice, 2014, pg. 188
[382] J Milas et al, Computer Law & Security Review 30, 2014, pg. 420
[383] K Hadjimatheou, Springer, 2017, pg. 43

what is called "wrongful criminalisation", as individuals are treated in the same manner as those who are involved in criminal activity, without sufficient grounds for doing so.[384]

Furthermore, connection between the right to be trusted and surveillance is not one limited to academic theory, and has been recognised in both political and legal spheres. For example in a report compiled by the UK House of Lords Constitution Committee on surveillance, it was noted by Professor Clive Norris that "[m]ass surveillance promotes the view … that everybody is untrustworthy. If we are gathering data on people all the time on the basis that they may do something wrong, this is promoting a view that as citizens we cannot be trusted".[385] Moreover, in a decision of the Romanian Constitutional Court on data retention, the Court noted that treating all citizens equally, regardless of whether they had committed or were likely to commit a crime, would be "likely to overturn the presumption of innocence and to transform a priori all users of electronic communication services or public communication networks into people susceptible of committing terrorism crimes or other serious crimes".[386] The European Parliament has also recognised this link, stating in their working report on US and EU surveillance programmes that "[t]he practice of untargeted, mass surveillance and the collection of bulk data of EU citizens may at least risk violating…the presumption of innocence" as it "leads to a shift in criminal law from its role of sanctioning specific acts on the basis of personal responsibility to reducing risks and identifying possible offenders, which can lead to all citizens, under continuous surveillance, being considered as suspects".[387]

These examples show that whilst the argument that the presumption is violated by mass surveillance is yet to be recognised before an international human rights body such as

[384] Ibid., pg.45
[385] House of Lords Constitution Committee, 2nd Report, *Surveillance: Citizens and the State*, 2009, at 107
[386] Decision no. 1258, 8th October 2009, Romanian Constitutional Court
[387] European Parliament Committee on Civil Liberties, Justice and Home Affairs, *Working Document 1 on the US and EU Surveillance programmes and their impact on EU Citizens fundamental rights,* 2013, at 3.6

the ECtHR, it may only be some time before Article 6 and other relevant provisions are used in this way. The increase in surveillance in the United Kingdom and Germany cannot be ignored, and must be challenged by all means necessary. The strict confinement of the presumption of innocence to the trial stage may currently deny such an approach, however through interpreting this protection as a "right to be trusted" or a "right not to be stigmatised as criminally suspicious", civil liberties advocates may be able to stifle any further increases in state monitoring. Whilst it is very likely that any further challenges will be based solely on the right to privacy, considering the impact that the use of investigative technologies have on criminal procedure rights, especially in the pre-crime context, is undoubtedly an argument that should be made.

Chapter 3: Evidentiary Rules and Electronic Evidence

i) Introduction

Whilst in the previous chapters, in following with the title of this work, the central point of discussion has been whether investigators' use of modern technology interferes with criminal procedure rights, at this point it becomes necessary to take a slight departure. As noted when analysing the conflict between surveillance practices and the presumption of innocence, in approaching issues concerning technology and its impact on citizens, it has been regarded common place in both legal theory and practice to make arguments under the right to private life. This is indeed often a successful endeavour, raising the question of whether the effort of claiming that these actions violate the right to a fair trial is truly beneficial. As was illustrated previously, showing that forced key disclosure infringes the privilege against self-incrimination will depend greatly on the specific facts of the case, and contending that surveillance violates the presumption of innocence remains for the time being a theoretical rather than practical solution.

Nevertheless, if we are to proceed with the premise that both of the above propositions will be successful, then the benefits of making such arguments become clear. Firstly, if domestic authorities are constrained by not only by privacy considerations, but also the right to a fair trial, then they will be further deterred from violating, and thus encouraged to follow, the criminal procedure frameworks for obtaining evidence. Secondly, arguing primarily under the aforementioned criminal procedure rights may, in addition to restricting the actions of the police at the point of interception, provide an exclusionary rule for any obtained evidence. This exclusion will be contrasted with the differing positions on the use of electronic evidence when it is shown to be unlawfully obtained under domestic law, or in violation of other civil liberties, most notably the right to privacy. Whilst the evidentiary rules of the United Kingdom, Germany, and the ECtHR all differ slightly in their approach, since

the implementation of the latter's jurisprudence into domestic law, a general trend can be shown throughout. What remains to be ascertained is whether the advantages gained through arguments based on criminal procedure rights are enough to justify this complete shift in approach when challenging the access to electronic evidence.

ii) The United Kingdom

At this current point in time, the United Kingdom's position on the admissibility of unlawfully obtained information, and evidence obtained contrary to fundamental rights, is predominantly dictated by the findings of the Strasbourg Court through the enforcement and obligations arising from the Human Rights Act 1998.[388] However, the present legal standard has also been largely influenced by common and statutory law, both of which significantly pre-date the 1998 Act and even the writing of the Convention itself. One predominant theme arising out of the common law, which remains pertinent to this day, is the rule that the unlawfulness of the collection of evidence will not in itself be a ground for exclusion.[389] Although some situations will inevitably result in the evidence being declared inadmissible, the mere fact that it is the result of improper or illegal conduct will not automatically lead to it being struck out.[390] The origins of this position stretch back to the 19th Century, where in the 1861 case of *R v. Leathem* it was held that "it matters not how you get it; if you steal it even, it would be admissible".[391] Although this cannot be claimed to remain as the current UK legal standard for admissibility, the restrictions that have been placed over time have been relatively minimal. For example in *R v. Christie* in 1914, the House of Lords stated that "in order to ensure a fair trial for the accused…evidence which, although admissible in law, has little value in its direct bearing upon the case, and might indirectly operate seriously to

[388] See page 85 below.
[389] B Emmerson et al, *Human Rights and Criminal Justice*, London, 2007, pg. 592
[390] N Monaghan, *Law of Evidence*, Cambridge, 2015, pg. 150
[391] *R v. Leathem*, (1861) 8 Cox CC 501

the prejudice of the accused, should not be given against him".[392] Despite the Lords acknowledging that some evidence should be excluded, this was restricted to solely where it was both of "little value" and seriously prejudicial.

The evidentiary rules were furthered expanded by the Privy Council in the 1955 case of *Kuruma v. R*, where it was held that when ruling on admissibility the issue is not how the evidence was obtained, but the relevance of its use in trial.[393] Lord Goddard set the common law standard, stating that "in a criminal case the judge always has a discretion to disallow evidence if the strict rules of admissibility would operate unfairly against an accused".[394] Despite temporary departures from this holding, such as in *R v. Payne* in 1963 where the Court of Appeal held that evidence obtained through trickery would be inadmissible, the rules set in *Christie* and *Kuruma* remained the position of the English courts on admissibility for a large part of the mid-20th Century.[395] With regard to electronic evidence obtained through the methods described in the previous chapters of this analysis, these holdings would mean that the violations of human rights involved in collection would be irrelevant, and instead the domestic court's decision would turn solely on what impact it had on proceedings.

The current common law standard was set in the 1979 House of Lords case of *R v. Sang*, in which the Court sought to provide greater clarity to the previous requirements.[396] This case concerned the defendant's conviction for trying to "utter counterfeit American banknotes", which he claimed he had been induced to do by an agent provocateur.[397] The defence of entrapment, normally relied on for such a claim, did not exist in English law, and therefore the Court had to consider whether the evidence should have been declared

[392] N Monaghan, *Law of Evidence*, Cambridge, 2015, pg. 150, *R v. Christie*, [1914] A.C. 563
[393] *Kuruma v. R*, [1955] A.C. 204
[394] Ibid.
[395] N Monaghan, *Law of Evidence*, Cambridge, 2015, pg. 151, *R v. Payne*, [1963] 1 W.L.R. 637
[396] *R v. Sang*, [1980] A.C. 402
[397] Ibid., 429

inadmissible due to its unlawful collection.[398] In his decision, Lord Diplock formed the present common law rule, stating that a "trial judge in a criminal trial has always a discretion to refuse to admit evidence if in his opinion its prejudicial effect outweighs its probative value".[399] However, crucially, Lord Diplock further qualified this ruling stating that this trial judge "has no discretion to refuse to admit relevant admissible evidence on the ground that it was obtained by improper or unfair means. The court is not concerned with how it was obtained".[400] Therefore, even where electronic evidence was obtained either unlawfully, or in violation of the Convention, the common law would not permit the trial judge to use his discretion to deem it inadmissible on this ground alone.

Nevertheless, the holding of *Sang* is not the sole exclusionary rule available in the United Kingdom. Defendants can additionally rely on Section 78 of the Police and Criminal Evidence Act 1984, which states that "[i]n any proceedings the court may refuse to allow evidence on which the prosecution proposes to rely to be given if it appears to the court that, having regard to all the circumstances, including the circumstances in which the evidence was obtained, the admission of evidence would have such an adverse effect on the fairness of the proceedings that the court ought not to admit it".[401] Whilst the principle of looking at the fairness of the trial as a whole mirrors that of the common law rule, the Court also has to explicitly examine how the evidence was obtained. Furthermore, although the *Sang* rule could be applied by judges at their discretion, Section 78 places an obligation on trial judges to take into account its provisions in all evidential matters. This was confirmed in the case of *R v. Mason* in 1987, where despite stating that the law did "no more than to re-state the power which the judges had at common law", the Court of Appeal further held that the trial judge

[398] Ibid., 420
[399] Ibid., 437
[400] Ibid.
[401] s78(1) Police and Criminal Evidence Act 1984

had failed to take regard of the deception practiced in obtaining a confession, and if he had he would have ruled the evidence inadmissible, therefore the proceedings could not be regarded as fair.[402]

The limitations of the Section 78 challenge were displayed in *R v. Sat-Bhambra*, where the Court of Appeal held that the Section ceased to have effect where the evidence had been declared admissible before a jury.[403] However under the 1984 Act, and as noted by the Court in *Sat-Bhambra*, in such situations the common law rule of *Sang* could still apply.[404] Section 82(3) states that "[n]othing in this Part of this Act shall prejudice any power of a court to exclude evidence (whether by preventing questions from being put or otherwise) at its discretion".[405] Through adding this qualification, suspects in the UK are provided with two opportunities to challenge the admissibility of evidence, firstly on the basis that it would have a seriously "adverse effect" on proceedings under the statute, and secondly, if the judge deems that its "prejudicial effect outweighs its probative value" through the common law.

In regards to the evidence relevant to this analysis, where it is obtained under surveillance laws or through key-disclosure provisions, the ability of the 1984 Act and the common law discretion to exclude the resulting information is not assured. Even if the previously argued self-incrimination and presumption of innocence arguments are used, the decision will ultimately come down to the discretion of the trial judge. However, following the coming into force of the Human Rights Act 1998, success in such arguments has become much more likely. Section 3 of the 1998 Act states that "[s]o far as it is possible to do so, primary legislation and subordinate legislation must be read and given effect in a way which is compatible with the Convention rights".[406] Therefore, when regarding the admissibility of

[402] *R v. Mason*, [1988] 1 W.L.R. 139
[403] N Monaghan, *Law of Evidence*, Cambridge, 2015, pg. 155. *R v. Sat-Bhambra*, (1989) 88 Cr. App. R. 59
[404] Ibid.
[405] s82(3) Police and Criminal Evidence Act 1984
[406] s3(1) Human Rights Act 1998

evidence under Section 78 of the 1984 Act, the Court would be under an additional statutory obligation to take into account any human rights based arguments. Furthermore, the Human Rights Act has also had an effect on the common law as Section 6 provides that "[i]t is unlawful for a public authority to act in a way which is incompatible with a Convention right".[407] The definition of public authority explicitly includes a "court or tribunal", which in turn means that when applying the *Sang* rule, the trial judge will also have to take into account any human rights arguments made by the parties.[408] In practical terms, this means that if the admission of certain forms of evidence would result in the violation of the right to a fair trial under Article 6 of the Convention, then the judge would be acting unlawfully if this did not influence his decision under the 1984 Act or the common law. [409]

Understandably, it could be argued that the findings of the Court will be entirely dictated by the jurisprudence of the ECtHR, which will be discussed in greater detail later in this chapter. However, as the UK Courts' decisions on admissibility remain predominantly dictated by national law, the domestic jurisprudence on this issue has particular nuances that differ slightly from that of the Strasbourg Court, and provide an interesting perspective on the conflict between the use of investigative technology and the right to a fair trial. In particular, UK case law has illustrated that whilst violations of the Convention will oblige the trial judge to consider human rights in regards to the evidence's admissibility, whether it will be struck out will depend greatly on the right in question. For example, there has been a general common law rule, as there is in several other jurisdictions, that any evidence obtained by torture should be regarded as inadmissible.[410] This was qualified by Lord Bingham in the case of *A and Others v. Secretary of State for the Home Department*, where he suggested that

[407] Ibid., s6(1)
[408] Ibid., s6(3)(a)
[409] B Emmerson et al, *Human Rights and Criminal Justice,* London, 2007, pg. 594
[410] Ibid., pg. 592

a distinction could perhaps be drawn between evidence obtained by torture, which would automatically be inadmissible, and practices that constitute "inhuman or degrading" treatment, which perhaps could be permitted due to its less serious infringement on fundamental rights.[411] Even though Article 3 had to be considered by the Court in making their decision, it did not automatically overrule their discretion.

Whilst this rights-specific approach to the exclusion of evidence has been shown in the holdings of several cases in the United Kingdom, the one right that has been shown to face the most stringent limitations is that often used in the context of electronic evidence: the right to privacy. For example in the case of *R v. P and Others*, the House of Lords had to consider whether evidence obtained by interception in a foreign country was admissible in the UK.[412] In their holding, the Lords found that even where Article 8 has been interfered with, this will not in itself require the evidence to be excluded, and instead Article 6 considerations under Section 78 of the 1984 Act must be the overriding consideration.[413] The limitations of Article 8 were further shown by the Court of Appeal in *R v. Mason et al*, where the suspects were covertly surveilled whilst in police custody, and the evidence obtained was used against them at trial.[414] The Court acknowledged that this surveillance interfered with Article 8 of the Convention, and could not be justified under the second paragraph as it was not in accordance with the law.[415] Nevertheless, they held that this "non-compliance with Article 8" did not mean that the tape-recordings could not be relied upon as evidence.[416]

[411] *A and Others v. Secretary of State for the Home Department (No 2)*, [2005] UKHL 71. B Emmerson et al, *Human Rights and Criminal Justice*, London, 2007, pg. 592
[412] *R v. P and Others*, [2000] UKHL 69
[413] B Emmerson et al, *Human Rights and Criminal Justice*, London, 2007, pg. 593
[414] *R v. Mason*, [2002] EWCA Crim 385 at [13] – [17]
[415] Ibid., at [73]
[416] Ibid., at [74]

Whilst it was acknowledged that the Court was under a legal obligation to provide a remedy to this violation, it did not have to result in exclusion.[417]

This was again confirmed by the Court of Appeal in *R v. Grant*, where the fact that the authorities had recorded the defendant's conversations in custody, contrary to Article 8 of the Convention, did not automatically result in the evidence's inadmissibility under UK law.[418] However, this case was distinguishable from that of *Mason*, as the exchange was between the defendant and his lawyer, and thus considered to be a privileged communication.[419] This in turn meant that the Court was not solely considering a breach of Article 8, but also Article 6, and thus the "fairness" of the trial was tarnished to such a degree that the evidence could not be held to be admissible.[420] Whilst arguments under the right to private life were limited in their effectiveness, when it could be shown that the investigation violated Article 6, the Court had no option but to deem the trial to be unfair, and to quash the use of the evidence. As stated by Lord Bingham in the case of *Kebilene*, "I can conceive of no circumstances in which, having concluded that a feature rendered the trial unfair, the court would not go on to find a violation of Article 6".[421] Therefore, contrary to the standard approach taken under the right to privacy, if the evidence was shown to be obtained in violation of the privilege against self-incrimination, or the presumption of innocence, then under UK law the applicants would also be granted the additional benefit of having the electronic evidence at issue excluded.

Nevertheless, the legislation on surveillance in the United Kingdom does provide for some evidentiary rules that will prevent information that is intercepted through surveillance from being disclosed before a court. In the Regulation of Investigatory Powers Act 2000,

[417] Ibid., at [75]
[418] *R v. Grant*, [2006] Q.B. 79
[419] Ibid.
[420] Ibid.
[421] *R v. Director of Public Prosecutions ex parte Kebeline and Others*, [2000] 2 A.C. 343

Section 17 prohibits any evidence that is obtained under the Act from being used in proceedings.[422] Section 56 of the Investigatory Powers Act 2016 replicates this, further excluding any "secondary information" gained from the interference.[423] This is notable, as it makes the United Kingdom the only common law country in the world to have an explicit exclusionary rule on all intercept evidence.[424]

Furthermore, whilst there are some exceptions provided to this rule in the legislation, they remain very limited. For example, under Schedule 3 of the Investigatory Powers Act, intercept evidence may be admitted if it is obtained with the consent of the suspect, or is sought to be used in the prosecution of an offence of unlawful interception.[425] Information obtained following surveillance practices such as eavesdropping, covert monitoring, or the placing of 'bugs' may also remain admissible, but this will depend on the circumstances of the case.[426] These exceptions do not stretch to cover any of the practices analysed in the previous chapter, and thus, for the purposes of the United Kingdom, the possibility of excluding evidence under arguments based on the presumption of innocence may be regarded as irrelevant.

Following the previous rhetoric of this analysis, it could be expected that such an exclusionary rule would be viewed as a positive, as the argumentation used in respect of the benefits of the right to a fair trial is attempting to achieve exactly this. However, the purpose of appealing for the exclusion of surveillance evidence is not solely to prohibit its use in Court, but also to restrict the authorities in their initial collection. Whilst the UK's exclusionary rule will prevent intercept evidence from being used in the prosecution of a

[422] s17(1) Regulation of Investigatory Powers Act 2000
[423] s56 Investigatory Powers Act 2016
[424] *Intercept Evidence*, Justice, Accessed via https://justice.org.uk/intercept-evidence/ on 27/10/2018
[425] Investigatory Powers Act 2016, Schedule 3 (2) – (3)
[426] Liberty, *Liberty's response to the Joint Committee on Human Rights*: "*Relaxing the Ban on the Admissibility of Intercept Evidence"*, February 2007, pg. 16

suspect, it fails to encourage the authorities to ensure that their surveillance operations are legal, proportionate, and in line with fundamental rights. As argued by Liberty, removing this exclusionary rule would "have the salutary effect of focusing the authorities' minds on the primacy that should be given to criminal investigations, prosecutions and trials over speculative, intelligence gathering fishing expeditions".[427] The need to admit some evidence on this ground has indeed been recognised by the UK Government, who in several reports have indicated that they may want to move towards such a standard, yet have failed to translate this into legislation.[428] Although allowing intercept evidence to become admissible may be seen to further threaten the rights of suspects, it will in turn ensure that the authorities are encouraged to remain within their boundaries during investigations, and where they do not, arguments under the right to fair trial will then act to exclude surveillance evidence as necessary.

iii) Germany

It could be expected that due to Germany's civil law based system, and having provisions governing admissibility fixed within the Code of Criminal Procedure, that their evidentiary regulations would be remarkably different from those of the United Kingdom. Indeed, due to the inquisitorial nature of the German system, the rules come into play a much earlier stage, restricting the authorities when the evidence is obtained.[429] Unlike the United Kingdom, the purpose of the German law on evidence is to protect the suspect from the authorities at the acquisition of the information, rather than regulating its use at trial. [430] As

[427] Liberty, *Liberty's Summary of the Investigatory Powers Bill for Second Reading in the House of Commons,* March 2016, pg. 11
[428] See *Intercept as Evidence*, HM Government, December 2014, CM 8989 and A Home, *The Use of Intercept Evidence in Terrorism Cases*, Home Affairs Section, 24th November 2011.
[429] J Ross, *Do Rules of Evidence Apply (Only) in the Courtroom? Deceptive Interrogation in the United States and Germany*¸ Oxford Journal of Legal Studies, Vol. 28, No. 3, 2008, pg. 445
[430] Ibid., pg. 472

noted by Jacqueline Ross, this approach "makes sense" for the German legal system, due to the trial being only one of the procedural phases "in the handling and sifting of evidence".[431]

However, the overarching principles governing the German evidentiary rules remain largely similar those of the United Kingdom, as despite the Code of Criminal Procedure setting the standards for the process, the trial judge is provided with a significant discretion in deciding what is to be admissible. The *Beweisverwertungsverbote*, or prohibitions of the use of evidence, form the rules of criminal procedure in this area of German Law.[432] This covers the rules set out in the Code of Criminal Procedure, which shall be discussed below, and also encompasses the two constitutional doctrines of the *Rechtsstaatsprinzip* and the *Verhältnismässigkeit*.[433] The *Rechtsstaatsprinzip*, or the principle of a state governed by the rule of law, provides that any evidence that has been obtained through brutality or deceit has to be declared inadmissible and excluded, in order to "preserve the purity of the judicial process".[434] The second doctrine, the *Verhältnismässigkeit*, Germany's principle of proportionality, requires judges to engage in a balancing process, on a case by case basis, to determine whether the defendant's personal privacy interests in the exclusion of evidence are outweighed by the seriousness of the offence.[435] This process, providing the German judiciary with the power to decide for themselves whether to admit evidence, largely resembles the aforementioned UK common law discretion of *Sang*.[436] Nevertheless, some theoretical differences remain.

[431] Ibid., pg. 473
[432] S Ast, *The Gäfgen Judgment of the European Court of Human Rights: On the Consequences of the Threat of Torture for Criminal Proceedings*, German Law Journal Vol. 11 No. 12, 2010, pg. 1403
[433] C M Bradley, *The Exclusionary Rule in Germany*, Indiana University, 1983, pg. 1034
[434] Ibid.
[435] Ibid.
[436] See page 83 above.

According to Stephan Ast, the jurisprudence of the German Courts has illustrated three purposes under threat if the evidentiary principles are violated.[437] Firstly, the rules act to "retain the legitimation of punishing".[438] If all evidence is admitted to court, no matter how it has been obtained, then the decision will be deemed unfair and the judicial system will lose its standing in society. As noted in the Federal Supreme Court's Judgment of 17th March 1983, the need for justice "does not compel the investigation of truth at any price".[439] The second principle put forward by Ast is that the German evidentiary rules seek to "find the truth and to render a just punishment". [440] In essence this stems from the historical prohibition on evidence being obtained through torture, which would often result in false confessions, and thus without proper evidentiary rules, the conviction and punishment would be both false and unjust. However, it is Ast's third and final principle that provides the most interesting purpose for this analysis, where he describes the *informationsbeherrschungrechte*.[441] This set of rights provide guarantees over when a suspect can be made to reveal information, and when they cannot.[442] For example, a person cannot be coerced to reveal information unlawfully, and if such a violation does occur, under the *Folgenbeseitigungsanspruch* the consequences of the act must be reversed, often meaning that the evidence must be declared inadmissible.[443] Furthermore, through the *Fernwirkung*, if this information was obtained in violation of a subjective right, such as the prohibition of torture, then any evidence arising from it must also be struck out, but only if it could not have been obtained in a legal way.[444]

However, despite the strong principled basis for the *Beweisverwertungsverbote*, this does not necessarily equate to Courts finding that any violations of these rules will result in

[437] S Ast, German Law Journal Vol. 11 No. 12, 2010, pg. 1403
[438] Ibid.
[439] Judgement of 17th March 1983, 4 StR 640/82, at [14]
[440] S Ast, German Law Journal Vol. 11 No. 12, 2010, pg. 1403
[441] Ibid.
[442] Ibid.
[443] Ibid.
[444] Ibid.

evidence being excluded. [445] For example, when looking at the *Rechtsstaatsprinzip*, the Court will first look at the legality of the search, and second whether the seizure was unlawful.[446] Whilst an unconstitutional seizure may automatically lead to the exclusion of the evidence, an unconstitutional search followed by a merely unlawful seizure will not necessarily have the same outcome. [447] Therefore under these rules, in a similar manner to the United Kingdom, the trial judge has a great degree of discretion in deciding whether electronic evidence can remain before the court.

As outlined above, in addition to the constitutional principles on the exclusion of evidence, the *Beweisverwertungsverbote* also encompasses the rules set out in the German Code of Criminal Procedure.[448] Section 261 of the Code provides the law on the free evaluation of evidence, stating that the "court shall decide on the result of the evidence taken according to its free conviction gained from the hearing as a whole".[449] This is often quoted in conjunction with Section 244(b), which provides that "[i]n order to establish the truth, the court shall, *proprio motu*, extend the taking of evidence to all facts and means of proof relevant to the decision".[450] As argued by Martin, this means that the principle of free evaluation of evidence simultaneously permits and binds the judge to evaluate all evidence regardless of how it was obtained.[451]

Nonetheless, the Code does explicitly prohibit certain types of evidence from being admitted, notably the "prohibited modes of examination" set out in Section 136a.[452] This Section prevents the authorities from administering on suspects "ill-treatment", "induced

[445] C M Bradley, *The Exclusionary Rule in Germany*, Indiana University, 1983, pg. 1039
[446] Ibid., pg. 1041
[447] Ibid.
[448] Ibid., pg. 1034
[449] s241 The German Code of Criminal Procedure, StPO
[450] s244(b) The German Code of Criminal Procedure, StPO
[451] G A Martin, *The Exclusionary Rule Under Foreign Law*, Journal of Criminal Law and Criminology, Volume 52 Issue 3, Article 5, 1962, pg. 277
[452] s136a The German Code of Criminal Procedure, StPO

fatigue", "physical interference", "drugs", "torment", "deception", "hypnosis", unlawful coercion, threats of measures not permitted under the statute, and "holding out the prospect of an advantage not envisaged by statute".[453] With regards to the admission of evidence, the provision holds that any "[s]tatements which were obtained in breach of this prohibition shall not be used even if the accused consents to their use".[454]

However, in situations where the authorities do not meet this standard of unlawfulness, yet have still violated the Code of Criminal Procedure through the taking of evidence without the proper legal or constitutional safeguards, the evidence will very rarely be excluded.[455] In fact, illegally obtained evidence will be presumed admissible in the absence of any statutory ban, such as that of Section 136a.[456] As noted by Bradley, "[t]he criminal will not automatically go free simply because the constable has blundered".[457] Instead, the Court will aim to reach the optimal balance between adhering to the Code, respecting the defendant's constitutional rights, and serving the interests of the prosecution of crime.[458] However, this balance will not always be easily achieved, and the judge may take more heed of the severity of the charged offence, rather than the extent to which the act of obtaining the electronic evidence infringes the Code of Criminal Procedure.[459] As stated by Kleinknecht-Miller, "[a]n irreparable procedural blunder which might be ignored in the interest of the public claim to a prosecution for murder, can in petty larceny cases ensue the inadmissibility of the evidence".[460] Therefore, if evidence obtained by surveillance is

[453] Ibid., s136(1)
[454] s136a(c) The German Code of Criminal Procedure, StPO
[455] C M Bradley, *The Exclusionary Rule in Germany*, Indiana University, 1983, pg. 1035
[456] G A Martin, Journal of Criminal Law and Criminology, Volume 52 Issue 3, Article 5, 1962, pg. 278
[457] C M Bradley, Indiana University, 1983, pg. 1035
[458] Ibid., pg. 1036
[459] Ibid.
[460] Ibid.

unlawful, yet was in pursuance of the investigation of a serious crime, then it is unlikely to be excluded by the German Courts.

There remains one final ground on which citizens can challenge the use of evidence, as German Law may require its exclusion even where it is relevant, competent, and lawful, simply because it violates their constitutional rights.[461] Under the German Basic Law, encroachment upon rights is only permitted when it is provided for by statute, which specifies the right which it seeks to restrict.[462] Through this logic, and as argued by Martin, this means that in the said statutes restricting the rights of individuals, German lawmakers could put in provisions explicitly prohibiting the use of any evidence obtained.[463] However, due to the "principle of the exploration of truth", which "demands the investigation, prosecution and just punishment of crimes through the use of all evidence available", this remains a relative rarity.[464] Indeed, the only statute analysed above with such provisions is the Article 10 Act, which provides that evidence obtained through the interception of communications may only be used if for the purposes of one of the crimes listed in s100a(2) of the Code of Criminal Procedure.[465] The effect of this provision was displayed in the *Der Spiegel* case, which concerned the monitoring of a former Government employee's phone who was believed to be the source of a leak.[466] Whilst the Government claimed that the surveillance was to "avert imminent threats to the free democratic constitutional order or the existence or security of the Federation", the Court held that the evidence could not be used unless it proved that someone

[461] C M Bradley, Indiana University, 1983, pg. 1033
[462] Article 19(1) Basic Law for the Federal Republic of Germany
[463] G A Martin, Journal of Criminal Law and Criminology, Volume 52 Issue 3, Article 5, 1962, pg. 281
[464] Ibid.
[465] Act on the Restriction of the Security of Correspondence, Postal, and Telecommunications 1968. s100a(2) The German Code of Criminal Procedure, StPO. C M Bradley, Indiana University, 1983, pg. 1055
[466] Judgement of 18th April 1980, BGH 2 StR 731/79 at [1]

was likely to commit, or had committed one of the aforementioned listed crimes.[467] The evidence could not be used to prosecute a lesser offence.[468]

Unlike the United Kingdom, the statutory exceptions in Germany remain rather limited, and therefore in order to uphold the principles of the Basic Law, as mandated by Article 1(3), the German Courts have to once again utilise their own discretion in deciding whether to exclude evidence.[469] The standard practice for this, according to Martin, is that the Court will exclude evidence "only in the few cases where it deems the violation of basic rights or state interests to be an especially serious one", and "in all other cases it permits the use of illegally or even unconstitutionally obtained evidence, only reserving to the judge a dissenting ruling in the scope of his free evaluation of evidence".[470] Whilst there are prohibitions on obtaining evidence contrary to the right to silence or in violation of human dignity, as enforced by the Code of Criminal Procedure, no other rights will automatically have superiority over the principle of exploration of truth.[471] As previously mentioned, the Article 10 statute also imposes limitations on the use of evidence obtained through its mandated practices, however this does not account for the obtaining of electronic evidence under other legislation, or where it is unlawfully collected. In such scenarios, in a similar manner to the United Kingdom, German lawyers and courts will often focus on whether the infringing act violated the right to privacy, enshrined under Articles 2(1) and 10 of the Basic Law.[472] Following the proportionality analysis employed by the German Courts for the Basic Law, if the privacy rights of the suspect are deemed to outweigh society's interest in the capture of the evidence and the prosecution of the offence, the evidence must be excluded

[467] Ibid., at [6]–[7]
[468] C M Bradley, Indiana University, 1983, pg. 1057
[469] Article 1(3) Basic Law for the Federal Republic of Germany
[470] G A Martin, Journal of Criminal Law and Criminology, Volume 52 Issue 3, Article 5, 1962, pg. 282
[471] Ibid., pg. 281
[472] Articles 2(1), 10 Basic Law for the Federal Republic of Germany

regardless of the legality of its seizure.[473] This was illustrated in the *Diary case*, which concerned the adultery trial of a school teacher who denied several allegations under oath, despite entries from her diary appearing to provide evidence to the contrary, and was thus convicted of perjury.[474] The Federal Court of Appeals held that despite the privacy rights of the accused not mandating the automatic exclusion of the evidence, the public interest in the prosecution of the minor offence "would not be so significant that it would absolutely dictate the resignation of the fundamental right of the defendants".[475]

However, this proportionality test is a double-edged sword, as often despite a substantial interference on the suspect's right to privacy, such as would occur through the new German "state trojan" laws outlined in the previous chapter, the fact that the authorities are investigating a serious crime will be likely to outweigh this interest, and thus the evidence will be admissible. Furthermore, whilst it is arguably clear whether an offence can be deemed 'serious', the same cannot be said for intrusions on the right to privacy. In order to shed a greater degree of light on this predicament, in the Judgement of 31st January 1973 the Federal Constitutional Court employed a *Dreistufentheorie*, or three tiered analysis, in explaining whether evidence should be excluded on privacy grounds.[476] The first sphere was described as encompassing evidence obtained in violation of the fundamental absolute rights of the Basic Law, such as the dignity of man, where "[e]ven overwhelming interests of the general public cannot justify an interference in the absolutely protected core area of private life", and thus an analysis of "proportionality does not take place".[477] No matter what the nature of the offence, the evidence could not be declared admissible. The second sphere described by the Court covered acts that still infringed on privacy and the right to free development of

[473] J Lehmann, *Legal systems in Germany: overview*, Thomson Reuters, 2018, pg. 5
[474] Judgement of 21st February 1964, BGHSt 19 325 at [1 – 6]
[475] Ibid., at [23]
[476] C M Bradley, Indiana University, 1983, pg. 1044
[477] Judgement of 31st January 1973, BVerfG 2 BvR 454/71 at [34]

personality under Article 2(1) of the Basic Law, but did not violate an absolute right.[478] This was held to include taped conversations, which as long as they did not interfere with the "inviolable" rights provided by the Basic Law, would be subject to a proportionality analysis to determine their status before the Court.[479] As acknowledged by the Constitutional Court, "as a community-bound citizen, everyone must accept state measures taken in the overriding public interest, with strict respect for the principle of proportionality, provided that they do not affect the inviolable sphere of private life".[480] In the final tier, where the privacy and personality rights of the suspect are not infringed, for example through the secret recording of a business meeting, the evidence cannot be excluded in a proportionality analysis, and thus will always be admissible.[481]

Following this, it can be argued that when the taking of electronic evidence is shown to infringe upon the right to privacy or personality, then this would fall into the second sphere, and would be automatically subject to a proportionality analysis, and not excluded outright. As with the United Kingdom, this illustrates the limitations of privacy arguments concerning the capture of electronic evidence, as even where the act is shown to have violated such a right, the admissibility of the evidence will inevitably come down to the seriousness of the offence. On the other hand, if the evidence is shown to be in violation of the privilege against self-incrimination or other criminal procedure rights under Section 136a of the Code, it will be excluded.[482]

With regards to surveillance evidence obtained in violation to the presumption of innocence, as argued in the second chapter, this becomes slightly more difficult to ascertain,

[478] Ibid., at [35]
[479] Ibid.
[480] Ibid.
[481] Ibid., at [41-42]
[482] s136a The German Code of Criminal Procedure, StPO

as it is a principle absent from the fundamental texts of German Law. [483] However, following the incorporation of the ECHR on 3rd September 1953, the presumption of innocence has worked its way into the criminal procedure laws of Germany, and now retains a status as high as it does in any other country.[484] The Constitutional Court provided the presumption will full constitutional status in the decision of 26th March 1987, which concerned the apportionment of the cost of proceedings after a private prosecution was dropped.[485] In their judgement, the Court held that the presumption of innocence was an "integral part of the Basic Law's principle of rule of law", the aforementioned *Rechtsstaatsprinzip*, and thus had "constitutional rank".[486] As noted by Weigend, the Court went even further in linking the presumption to the fundamental rights of Germany, where they found it to be a "self-evident consequence" of a criminal-law order "whose contents and boundaries are defined by the precept of respect for human dignity".[487] Therefore, it can be argued that if the collection of evidence by surveillance was shown to violate the presumption of innocence, it would be treated by the Courts in a similar manner to that of violations of human dignity and other absolute rights, and will be excluded under the first sphere of the Judgement of 31st January 1973.[488] Even if the Court does not stretch as far as to provide the presumption with the status of a fundamental right, any proportionality analysis will require a particularly serious crime to render the evidence admissible, as in the words of Weigend, the "measures must be permissible and proportional even with respect to an innocent person".[489]

Unfortunately, in a similar manner to the United Kingdom, there is no current jurisprudence of the German courts in which electronic evidence has been excluded on the

[483] T Weigend, *Assuming that the Defendant Is Not Guilty*: The Presumption of Innocence in the German System of Criminal Justice, Crim Law and Philosophy, Springer, 2014, pg. 286
[484] Ibid.
[485] Judgement of 26th March 1987, 74 BVerfGE 358 at [370]
[486] Ibid., at B, I, 1(a)
[487] Ibid., T Weigend, Crim Law and Philosophy, Springer, 2014, pg. 286
[488] Judgement of 31st January 1973, BVerfG 2 BvR 454/71 at [34]
[489] T Weigend, Crim Law and Philosophy, Springer, 2014, pg. 296

basis of the presumption of innocence. However, we can instead look to the decisions of the ECtHR, which have been shown to have a growing influence on German evidentiary rules. The findings of the Strasbourg Court on the admission of evidence will be discussed in great detail below, but at this point one judgement is of particular relevance in how it shaped and altered the approach of the German judiciary. The case of *Gäfgen v. Germany* concerned the interrogation of a suspect to a kidnapping, in which the applicant was threatened with "considerable physical pain" in the event that he did not disclose the location of the young boy to the authorities.[490] In their decision, the Court found that this amounted to inhuman treatment, and therefore violated Article 3 of the Convention.[491] However, it was the applicant's claims brought under Article 6 that are of particular interest, where he argued that the German trial court should have found inadmissible not only the statements made under the threat of torture, but also any evidence arising therefrom.[492] The Court held that "incriminating real evidence obtained as a result of acts of violence, at least if those acts had to be characterised as torture, should never be relied on as proof of the victim's guilt, irrespective of its probative value".[493] The impact of this judgement has been documented by Ast, who notes that not only was this a substantial step in the jurisprudence of the Strasbourg Court, but it also played a significant part in amending the German law on excluding evidence.[494] Therefore, it is clear that in order to properly adduce whether arguments made under criminal procedure rights could have a greater impact on excluding electronic evidence, it is necessary to look into the decisions of the ECtHR. Although the evidentiary rules of both the United Kingdom and Germany are steeped their own principles of domestic

[490] *Gäfgen v. Germany*, Application no. 22978/05, 2010, § 15
[491] Ibid., § 132
[492] Ibid., § 136
[493] Ibid., § 167. However, as will be discussed below, this did not lead to the Court finding a violation of Article 6 (§ 188).
[494] S Ast, German Law Journal Vol. 11 No. 12, 2010, pg. 1402

law, their progression and adaptation over the past 30 years, and hopefully for the considerable future, will be determined as much from Strasbourg as London or Karlsruhe.

iv) ECtHR and Admissibility of Evidence

The European Court of Human Rights, as discussed in the previous chapters of this analysis, acts to ensure that the rights enshrined in the Convention are complied with in the 47 member states. However, in performing their supervisory role, the Court is careful not to encroach to a degree greater than what is necessary to achieve this, in following with the "fundamentally subsidiary role of the Convention".[495] Closely related to this principle is another unique structural feature of the Strasbourg Court, named the "fourth instance" doctrine.[496] This doctrine provides that the ECtHR is not to act as a Court of Appeal, and that it is not their task "to review the observance of domestic law by the national authorities".[497] The Court has extended this principle to cover issues relating to the determination of the guilt of an applicant before national law, where they refuse to interfere with the domestic court's findings on the merits.[498] Therefore, when questions relating to the admissibility of evidence are brought to Strasbourg, it has been a longstanding response of the Court to declare that "in principle it is for national courts to assess the evidence gathered by them".[499] Nevertheless, this is almost always caveated by the qualification that it is instead the task of the Court "to ascertain whether the proceedings considered as a whole, including the way in which the evidence was taken, were fair".[500] This leaves the open the possibility for the ECtHR to make rulings on admissibility of evidence, where they deem that it has been obtained in such a way as to jeopardise the right to a fair trial, mandated under Article 6 of the Convention. The need

[495] *Hatton and Others v. The United Kingdom*, Application no. 36022/97, 2003, § 97
[496] R Reed & J Murdoch, *Human Rights Law in Scotland*, 3rd Edition, Bloomsbury, 2011, pg. 291
[497] *Winterwerp v. the Netherlands*, Application no. 6301/73, 1979, § 46
[498] S Trechsel, *Human Rights in Criminal Proceedings*, Oxford, 2005, pg. 174
[499] *Goktepe v. Belgium*, Application no. 50372/99, 2005, § 25
[500] *Bernard v. France*, Application no. 22885/93, 1998, § 37

to perform this function was noted in 2007 by the then President of the Court, Jean-Paul Costa, where he stated that "[a]lthough we must not set ourselves up as a fourth instance rehearing what has already been heard in the domestic courts, we do have a duty to oversee the requirements of fair trial as guaranteed by Article 6 of the Convention".[501]

Compared to the evidentiary rules of the previous jurisdictions, through determining admissibility on whether it affects the fairness of proceedings as a whole, it is substantially more difficult to predict when the ECtHR will rule that evidence should have been excluded. Instead, it is perhaps easier to adduce the situations in which the Court will not find issue with the way in which the information was obtained. For example in the case of *Schenk v. Switzerland,* the Court held that they could not "exclude as a matter of principle and in the abstract that unlawfully obtained evidence of the present kind may be admissible" and that they only had to "ascertain whether Mr Schenk's trial as a whole was fair".[502] As noted by Goss, the *Schenk* judgment creates a "false dichotomy", as it makes it unclear whether the job of the ECtHR is to rule on the admissibility of evidence to adduce if the trial is fair, or whether they should refrain from looking at admissibility at all even when checking the fairness as a whole.[503] The only part of clarity that the Court do provide is that the mere fact that evidence was obtained unlawfully will not have an immediate exclusionary effect or lead to a violation of the Convention.

Unfortunately, in a similar manner to the United Kingdom and Germany, the jurisprudence of the ECtHR also provides little clarity on whether the violation of a Convention right will automatically require the exclusion of the obtained evidence. In fact, the only right which will almost always require the exclusion is of evidence is Article 3,

[501] Council of Europe, *The role of Supreme Courts in the domestic implementation of the European Convention on Human Rights,* Proceedings of the Regional Conference Belgrade, 2008, pg. 21
[502] *Schenk v. Switzerland,* Application no. 10862/84, 1988, § 46
[503] R Goss, *Criminal Fair Trial Rights,* Oxford, 2014, pg. 60

which provides the prohibition of torture, inhuman or degrading treatment or punishment.[504] This was illustrated in the case of *Jalloh v. Germany* which, as described in the first chapter, concerned the forced administration of an emetic to a suspected drug dealer, after he swallowed a small bag of cocaine.[505] The obtained evidence was then relied on for his conviction in the domestic court proceedings.[506] In their decision, as the applicant had been subject to measures that had caused him "both physical pain and mental suffering", the ECtHR found a violation of Article 3 on the basis of inhuman and degrading treatment.[507] When then considering whether the evidence should have been excluded at trial, the Court stated that "incriminating evidence – whether in the form of a confession or real evidence – obtained as a result of acts of violence or brutality or other forms of treatment which can be characterised as torture – should never be relied on as proof of the victim's guilt, irrespective of its probative value".[508] If used before the domestic court, this would have the effect of rendering the trial as a whole unfair, "irrespective of the seriousness of the offence allegedly committed, the weight attached to the evidence and the opportunities which the victim had to challenge its admission and use at his trial".[509] By denying any form of proportionality analysis to the admissibility of evidence obtained in violation of Article 3, this created a significantly stringent evidentiary rule compared to that of the domestic principles of the UK and Germany. As acknowledged by Goss, the holding of this judgment resulted in member states being obliged to declare certain evidence as inadmissible, irrespective of the circumstances of the case, if they wished to comply with the Convention and the jurisprudence of the ECtHR.[510]

[504] Article 3 ECHR
[505] *Jalloh v. Germany*, Application no. 54810/00, 2006, § 14
[506] Ibid., § 20
[507] Ibid., §§ 82, 83
[508] Ibid., § 105
[509] Ibid., § 106
[510] R Goss, *Criminal Fair Trial Rights,* Oxford, 2014, pg. 61

The findings of the Court in *Jalloh* were reinforced and built upon four years later in the aforementioned case of *Gäfgen*.[511] In finding that the obtained statement could not be used at trial, the Court provided justification for their creation of an exclusionary rule, which was an area of the law that they had previously explicitly avoided. In countering arguments over the need to punish and prosecute certain offenders, the Court stated that there was a corresponding "vital public interest" in the preservation of the judicial process, and further that the "the admission of evidence obtained by conduct absolutely prohibited by Article 3 might be an incentive for law-enforcement officers to use such methods notwithstanding such absolute prohibition".[512] However, the *Gäfgen* judgement refrained from expanding the exclusion of evidence to a 'fruit of the poisonous tree' doctrine, where any information obtained as a result of the previously inadmissible evidence would also have to be automatically struck out.[513] Instead, the Court stated that they would determine whether this resulting evidence "had an impact on his or her conviction or sentence", the absence of a finding of which, as in the case of the applicant, would lead to the ECtHR permitting its use.[514]

Despite this, it is highly unlikely that the collection of electronic evidence could ever be argued to be obtained contrary to Article 3 of the Convention. Therefore, it is necessary to look into the jurisprudence of the Court regarding the evidentiary standing when a violation of the right to privacy, or the criminal procedure provisions of the right to a fair trial, has been previously found. Where the Court has found a violation of the right to private and family life, they often will have engaged themselves in a proportionality analysis under the second paragraph of the provision, and thus have decided that the legitimate aim pursued was

[511] *Gäfgen v. Germany*, Application no. 22978/05, 2010
[512] Ibid., §§ 175, 178
[513] Ibid., § 178
[514] Ibid.

not enough to justify the level of the intrusion. However, even where this has been found, it will not automatically lead to the exclusion of the evidence, and once again the Court will have to decide on the facts of the case.[515] This was illustrated in *Schiechelbauer v. Austria*, a relatively early case before the Commission, where they held that even though the intercept of a telephone interfered with Article 8, it was not enough to render the trial as a whole unfair.[516]

Nevertheless, it was in the case of *Khan v. the United Kingdom* that the Court truly set the standard on the admissibility of intercept evidence that has been found to be obtained in violation of Article 8.[517] This case concerned the audio surveillance of the applicant in which he admitted to being complicit in the import of drugs.[518] The trial judge ruled this evidence admissible, and the applicant was convicted on that basis.[519] The ECtHR found this action to be in violation of Article 8, as the investigatory act clearly interfered with the applicant's right to a private life, and was not "in accordance with law".[520] In light of the Court's previous jurisprudence, it could have been predicted that due to the recording constituting the predominant piece of evidence used in the applicant's conviction, this would inevitably render the trial as a whole unfair, and thus constitute a violation of Article 6. This was indeed acknowledged by the Government in their submissions, however they qualified this by stating that "where there is strong evidence to prove the involvement of a person in a serious crime, then there is a strong public interest in admitting it in criminal proceedings, even if it is the only evidence against the accused".[521] Surprisingly, the Court took a similar line to the Government, finding no violation of Article 6, as the trial as a whole was regarded to be

[515] B Emmerson et al, *Human Rights and Criminal Justice,* London, 2007, pg. 583
[516] *Scheichelbauer v. Austria,* Application no. 2645/65, Commission, 1969. B Emmerson et al, London, 2007, pg. 583
[517] *Khan v. The United Kingdom,* Application no. 35394/97, 2000
[518] Ibid., §§ 9, 10
[519] Ibid., § 12
[520] Ibid., §§ 25, 28
[521] Ibid., § 30

fair.[522] In reference to the evidence being the sole piece used, the Court stated that "the relevance of the existence of evidence other than the contested matter depends on the circumstances of the case" and that as "the tape recording was acknowledged to be very strong evidence…there was no risk of it being unreliable", and the need for any supporting evidence was "correspondingly weaker".[523] Furthermore, the Court gave substantial weight to the powers of the domestic UK Courts to exclude evidence under the aforementioned Section 78 rule, going as far to state that "it is clear that, had the domestic courts been of the view that the admission of the evidence would have given rise to substantive unfairness, they would have had a discretion to exclude it under section 78 of PACE".[524] This essentially means that if the obtaining of surveillance evidence is shown to be in violation of Article 8, and the domestic courts do not find it to be contrary to national rules of admissibility, then the ECtHR will also not require its exclusion. The controversial nature of this holding was reflected clearly in the partly dissenting opinion of Judge Loucaides, who stated that "I cannot accept that a trial can be "fair", as required by Article 6, if a person's guilt for any offence is established through evidence obtained in breach of the human rights guaranteed by the Convention".[525]

The holding of the Court, despite its criticisms, was replicated in the later case of *P.G. and J.H. v. the United Kingdom*, which also concerned covert audio surveillance of the applicants, the findings of which were used in their later conviction for conspiracy to commit armed robbery.[526] This evidence was not obtained in line with domestic law, and therefore the ECtHR had no difficulty in finding a violation of Article 8.[527] Nevertheless, in following with

[522] Ibid. § 37
[523] Ibid.
[524] Ibid., § 39
[525] Ibid., Partly Concurring Partly Dissenting Opinion of Judge Loucaides
[526] *P.G. and J.H. v. The United Kingdom*, Application no. 44787/98, 2001, §§ 10, 22, 23
[527] Ibid., § 38

the precedent set by *Khan*, the Court found that the use of the evidence at trial by the prosecution did not violate Article 6, as the recordings were "not the only evidence against the applicants" and because they had "ample opportunity to challenge both the authenticity and the use of the recordings".[528] Once again a source of clarity came in the form of the dissenting opinion, this time from Judge Tulkens, who asked "[w]ill there come a point at which the majority's reasoning will be applied where the evidence has been obtained in breach of other provisions of the Convention, such as Article 3, for example? Where and how should the line be drawn? According to which hierarchy in the guaranteed rights?".[529]

The answer to Judge Tulkens' first question was, as previously discussed, clarified in the cases of *Jalloh* and *Gäfgen*, as the Court has set a standard that any evidence obtained in violation of Article 3 must be declared inadmissible.[530] In regards to the second and third queries, concerning the hierarchy of guaranteed rights, all that is clear from the above jurisprudence is that violations of Article 8 certainly do not sit at the top. Indeed, this has also been shown to be the case in the domestic jurisdictions of the United Kingdom and Germany, where arguing that evidence has been obtained in violation of the right to privacy rarely leads to its exclusion. It is for this reason that this analysis claims that there is a second purpose to using the arguments set out in the previous two chapters. If the authorities are shown to have acted contrary to the privilege against self-incrimination or the presumption of innocence, not only will they face the domestic consequences for such an action, but the obtained evidence will further be excluded from use in a trial. It must be acknowledged that in order to achieve the above, the applicant will have to succeed in one of the various tests set out in the above chapters, which will be no mean feat. However in doing so, they will also show that the

[528] Ibid., § 79
[529] Ibid., Partly Dissenting Opinion of Judge Tulkens
[530] See pages 103 and 104 above.

investigation was completed contrary to the right to a fair trial, and thus the use of the evidence will automatically lead to the trial being deemed unfair as a whole.

This was illustrated in the above case of *Jalloh v. Germany*, where although the Court focused on the Article 3 violation, they also stated that would "have been prepared to find that allowing the use at the applicant's trial of evidence obtained by the forcible administration of emetics infringed his right not to incriminate himself and therefore rendered his trial as a whole unfair".[531] The benefits of such arguments were also shown in *Allan v. the United Kingdom*, where the police obtained a confession from the applicant in a similar manner to that in *Khan*: by covert audio surveillance.[532] However, in contrast to that case, Mr Allan's statements were not spontaneous, and were instead the result of repeated questioning by a police informant who was wearing a hidden recording device.[533] Consequently, the applicant did not have to rely solely on bringing his case under Article 8, of which the Court found a violation, and could also claim that the authorities' actions violated his right not to incriminate himself.[534] The Court found little difficulty in siding with the arguments of the applicant, stating that the evidence could be regarded "as having been obtained in defiance of the will of the applicant" and thus "its use at trial impinged on the applicant's right to silence and privilege against self-incrimination".[535]

Overall, it can thus be claimed that in addition to restricting the authorities at the point of capture, using criminal procedure rights to challenge practices of obtaining electronic evidence can also have a significant effect in restricting its use in the trial as a whole. Although there have been some minor differences in the exclusionary rules of the jurisdictions covered, one central theme has remained constant throughout; evidence is far

[531] *Jalloh v. Germany*, Application no. 54810/00, 2006, § 122
[532] *Allan v. The United Kingdom*, Application no. 48539/99, 2002, §§ 13, 14
[533] Ibid., §§ 14, 52
[534] Ibid., §§ 36, 37
[535] Ibid., § 52

more likely to be excluded if shown to be obtained in violation of the right to a fair trial than the right to privacy. Whilst there are indeed some instances where arguments based on privacy right will rule out the use of the obtained information, or a statutory provision will exclude it outright, domestic and international jurisprudence on this area has proven that this will often be determined on a case by case basis. In the regulation of the practices of obtaining electronic evidence, which due to modern technology now can contain the most personal of details about an individual, such subjectivity and discretion cannot be deemed to be a strong enough deterrent for the authorities. In a state governed by the rule of law it must be accepted that the authorities should be able to detect, investigate, and punish criminal offences, however there must also be limitations on how this is achieved. As acknowledged in the dissenting opinion of the *Khan* judgment, "[i]f violating Article 8 can be accepted as "fair" then I cannot see how the police can be effectively deterred from repeating their impermissible conduct".[536] Therefore, utilising the criminal procedure rights discussed above to challenge the interception of electronic information may, in addition to assisting the suspects to a crime, help the functioning of society as a whole.

[536] *Khan v. The United Kingdom*, Application no. 35394/97, 2000, Partly Concurring Partly Dissenting Opinion of Judge Loucaides

Conclusion

The purpose of this thesis was to assess whether obtaining electronic information in investigations interferes with suspects' criminal procedure rights. In light of the above, this question can be answered in the affirmative. Whether taken through the forced disclosure of a password, or remotely through online and mobile surveillance, it is clear that in addition to infringing upon the right to privacy, these actions will also have a considerable impact upon criminal procedure liberties. Outside the context of a court, restrictions based upon the right to a fair trial become understandably more difficult to implement, yet there are definitely signs of an expansion of such protections to individuals involved at any stage the criminal process, including those only affected during the investigation.

In the first chapter it was concluded that that the use of key disclosure provisions, predominantly employed in the United Kingdom, has had a significant impact on the privilege against self-incrimination. Through forcing an individual to unlock their electronic device under the threat of criminal sanction, they are consequently compelled to incriminate themselves. The domestic and international judicial opinion on this issue was shown to remain largely unclear, as courts have taken different, and often contradictory, views on whether this violates the privilege. As was discussed, the human rights implications of such actions will be largely dependent on the specific facts of the case, including the nature of the offence suspected, and the form of encryption present. Particular concern was raised with regards to new devices which utilise fingerprint and facial recognition technology, and despite providing users with greater accessibility to their information, have consequently granted investigating authorities with a human rights compliant loophole to get around the constraints of the privilege.

The impact of modern technology on criminal procedure rights was also at issue in the second chapter, where it was demonstrated that the increasing amount of personal data stored

on internet connected appliances has presented states with greater opportunities to monitor their citizens' activities. Although the United Kingdom and Germany have not been alone in taking advantage of these technological advances, their vast expansion of legislative provisions permitting the surveillance of individuals, and particularly of those not suspected to have committed a crime, cannot be ignored. Through shifting the purpose of criminal investigations from reactive to predictive, the domestic policing authorities have utilised the highly intrusive technology available to them in the aim of preventing crime prior to its commission. This has been authorised through new domestic legislation, which under the veil of increasing regulation of surveillance practices, has additionally expanded the use of untargeted and predictive monitoring. It is in these actions that it was argued that the right to a fair trial, and specifically the presumption of innocence, was interfered with. In treating innocent citizens as though they are criminals, or at the very least suspects, both the United Kingdom and Germany have undermined this fundamental criminal procedure right, and overstepped the boundaries of what can be accepted in domestic investigations. However, as was illustrated through the jurisprudence of the ECtHR, it is likely that such appeals will for the time being remain more of a theoretical consideration, due to the strict confinement of the presumption to after the provision of a criminal charge.

Despite this, these are undoubtedly arguments that should be attempted, especially due to the limitations of the standard approach taken under the right to privacy. As was illustrated in the third and final chapter, although privacy considerations remain an important means of restricting the powers of the state in accessing electronic information, they often fail to guarantee that the evidence obtained will not be used at trial. All three of the jurisdictions covered highlighted this deficiency, as even where the authorities are shown to have acted unlawfully under domestic law, or in violation of the privacy right, the decision on whether to exclude evidence will remain fully in the discretion of the trial judge. On the other hand,

when the evidence was argued to be taken in a manner that infringed the privilege against self-incrimination, the presumption of innocence, or indeed any other aspect of the right to a fair trial, this would often result in its immediate exclusion. It is at this point where this work departs from earlier research in this area, as even though conflict between the aforementioned practices and criminal procedure rights has been previously analysed, the true benefit to the individual in using such arguments has been notably absent. Utilising criminal procedure reasoning to restrict the state at the point of capturing electronic evidence will undoubtedly be effective, however it is this later exclusionary rule that will ensure that the investigating authorities are deterred from acting in violation of their own national laws, and more importantly, the suspect's fundamental rights.

It should be noted, however, that this thesis does not contend that the domestic authorities should be prohibited from utilising all the technology available to them to prevent, investigate, and punish those involved in criminal offences. It is inconceivable to suggest that investigators should have to rely on traditional means of policing when an increasing amount of the planning and commission of criminal activity is occurring through the use of modern technology. The regulated surveillance of criminal suspects must be tolerated, as it can be a crucial tool in the prevention of serious offences and terrorist activity. As was argued in relation to the United Kingdom's ban on intercept evidence, a complete prohibition on the use of all technology in criminal investigations will not necessarily make the authorities more human rights compliant. Instead, a line must be reached whereby investigators can effectively prosecute crime under strict regulation, ensuring a balance between protecting innocent citizens, and adhering to the fundamental rights of suspects.

Nevertheless, when these investigatory practices begin to affect the lives of innocent individuals, justifications based on the prevention of crime cannot be accepted. For example, criminal justice concerns cannot legitimise forcing an individual to hand over the password to

their phone, simply because they are reading a certain book, or reserve a seat on a specific flight. Furthermore, the potential of preventing an unknown criminal offence cannot be used to defend the indiscriminate and widespread surveillance of a whole sector of the population, a practice now utilised by the United Kingdom and Germany. It could be argued that the above human rights considerations would be served by the longstanding position to challenge these acts under the right to privacy, as those who are innocent will be unlikely to directly benefit from the exclusionary rule granted under the right to a fair trial. However, there are two primary reasons why this should not be deemed sufficient.

Firstly, through knowing that obtaining electronic evidence contrary to criminal procedure rights will automatically lead to its exclusion, investigators will be deterred from conducting these practices outright, thus benefitting both those who may be legitimate suspects to an offence, and those who are completely innocent. The risk of jeopardising an entire investigation will ensure that the authorities stays within their authorised legal boundaries, even where engaging in preventive policing. Secondly, arguments based solely on the right to privacy have been used to challenge the investigative techniques discussed for a considerable period of time, yet the legal provisions of the United Kingdom, Germany, and a large amount of the other member states of the Council of Europe, have not become more human rights compliant. Applicants and petitioners have successfully argued for decades that mass surveillance and the interception of personal information violates their privacy rights, and although transparency may have increased, the offending investigative practices employed by the states have remained, and in some cases expanded. Therefore, it is clear that there needs to be a considerable shift in the type of arguments used by civil liberties advocates to prevent the further development of these powers. In the opinion of this thesis, challenging on the basis of criminal procedure rights could potentially be the answer.

Bibliography

Case Law

The United Kingdom

A and Others v. Secretary of State for the Home Department (No 2), [2005] UKHL 71
Kuruma v. R, [1955] A.C. 197
R v. Christie, [1914] A.C. 545
R (David Miranda) v. Secretary of State for the Home Department, [2016] EWCA Civ 6
R (Davis & Watson) v. Secretary of State for the Home Department, [2018] EWCA Civ 70
R v. Director of Public Prosecutions ex parte Kebeline and Others, [2000] 2 A.C. 326
R v. Grant, [2006] Q.B. 60
R v. Leathem, (1861) 8 Cox CC 498
R v. Mason, [1988] 1 W.L.R. 139
R v. Mason, [2002] EWCA Crim 385
R v. P and Others, [2000] UKHL 69
R v. Payne, [1963] 1 W.L.R. 637
R v. S & Anor, [2008] EWCA Crim 2177
R v. Sang, [1980] A.C. 402
R v. Sat-Bhambra, (1989) 88 Cr. App. R. 55
R (K) v. Secretary of State for the Home Department, CO 10027/2011
R (on the application of Davis) v Secretary of State for the Home Department, [2015] EWHC 2092 (Admin)
Woolmington v DPP, [1935] UKHL 1

Germany

Judgement of 4th April 2006, 115 BVerfGE 320
Judgement of 14th July 1999, 100 BVerfG 313
Judgement of 17th March 1983, 4 StR 640/82
Judgement of 18th April 1980, BGH 2 StR 731/79
Judgement of 21st February 1964, BGHSt 19 325
Judgement of 26th March 1987, 74 BVerfGE 358
Judgement of 27th July 2005, 113 BVerfGE 348, 392
Judgement of 31st January 1973, BVerfG 2 BvR 454/71
Oberverwaltungsgericht NRW [Higher Administrative Court of NRW], June 22, 2017, docket no. 13 B 238/17.

European Court of Human Rights

Allan v. The United Kingdom, Application no. 48539/99, 2002
Allenet de Ribemont v. France, Application no. 15175/89, 1995
Barberà, Messegué and Jabardo v. Spain, Application no. 10590/83, 1988
Beghal v. The United Kingdom, Application no. 4755/16, Communicated Case, 2016
Bernard v. France, Application no. 22885/93, 1998
Big Brother Watch and Others v. The United Kingdom, Application no. 58170/13, 2018
Khan v. The United Kingdom, Application no. 35394/97, 2000
Funke v. France, Application no. 10828/84, 1993
Gäfgen v. Germany, Application no. 22978/05, 2010
Goktepe v. Belgium, Application no. 50372/99, 2005
Ibrahim and Others v. The United Kingdom, Application no. 50514/08, 2016

Klass and Others v. Germany, Application no. 5029/71, 1978
Hatton and Others v. The United Kingdom, Application no. 36022/97, 2003
Heaney and McGuinness v. Ireland, Application no. 34720/97, 2000
Ilgar Mammadov v. Azerbaijan, Application no. 15172/13, 2014
Jalloh v. Germany, Application no. 54810/00, 2006
John Murray v. The United Kingdom, Application no. 18731/91, 1996
Lingens v. Austria, Application no. 8803/79, 1982
Malone v. The United Kingdom, Application no. 8691/79, 1984
Minelli v. Switzerland, Application no. 8660/79, 1983
O'Halloran and Francis v. The United Kingdom, Application no. 15809/02, 2009
P.G. and J.H. v. The United Kingdom, Application no. 44787/98, 2001
Roman Zakharov v. Russia, Application no. 47143/06, 2015
S. and Marper v. The United Kingdom, Application no. 36562/04, 2008
Salabiaku v. France, Application no. 10519/83, 1988
Saunders v. The United Kingdom, Application no. 19187/91, 1996
Scheichelbauer v. Austria, Application no. 2645/65, Commission, 1969
Schenk v. Switzerland, Application no. 10862/84, 1988
Szabó and Vissy v. Hungary, Application no. 37138/14, 2016
Telfner v. Austria, Application no. 33501/96, 2001
Weh v. Austria, Application no. 38544/97, 2004
Winterwerp v. the Netherlands, Application no. 6301/73, 1979

European Court of Justice
*Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others***,** Joined Cases C-293/12 and C-594/12, 8th April 2014
Secretary of State for the Home Department v Tom Watson, Joined Cases C-203/15 and C-698/15, 21st December 2016

United States of America
Bell v. Wolfish, 441 U.S. 583 (1979)
Commonwealth of Virginia v. Baust, 89 Va. Cir. 267 (2014)
Fisher v. United States, 425 U.S. 411 (1976)
In re Application for a Search Warrant, 236 F.Supp.3d 1066 (2017)
In Re Boucher 2007 WL 4246473 (2009)
Murphy v. Waterfront Commission of N.Y. Harbour, 378 US 55 (1964)
Olmstead v. United States, 277 U.S. 473 (1928)
Riley v. California, 134 S. Ct. 2489 (2015)
State of Florida v. Stahl, 206 So.3d 124 (2016)
State of Minnesota v. Diamond, 2018 WL 443356 (2018)
United States v. Hubbell, 530 U.S. 27 (2000)
United States v. Kirschner, 823 F. SUPP. 2d 665 (2010)

Inter-American Court of Human Rights
Case of Escher et al. v. Brazil, Judgment of July 6 2009, IACtHR

Romanian Constitutional Court
Decision no. 1258, 8th October 2009, Romanian Constitutional Court

Legislation

The United Kingdom
Criminal Evidence Act 1898 c. 36
Data Retention and Investigatory Powers Act 2014 c. 27
Human Rights Act 1998 c. 42
Investigatory Powers Act 2016 c. 25
Police and Criminal Evidence Act 1984 c. 60
Regulation of Investigatory Powers Act 2000 c. 23
Terrorism Act 2000 c. 11

Germany
Act for Foreign-Foreign Signals Intelligence Gathering of the Federal Intelligence Service 2016
Act Introducing a Storage Obligation and a Maximum Retention Period for Traffic Data 2015
Act on the Restriction of the Security of Correspondence, Postal, and Telecommunications 1968
Act to Adapt Data Protection Law to Regulation (EU) 2016/679 and to Implement Directive (EU) 2016/680 (DSApUG-EU) of 30 June 2017
Act to Make Criminal Proceedings More Effective and Practicable 2017
Basic Law for the Federal Republic of Germany
BVerfG, Order of the First Senate of 14 July 1999 – 1 BvR 2226/94
The German Code of Criminal Procedure, StPO

International Legislation
CCPR General Comment No. 16: Article 17 (Right to Privacy), UN Human Rights Committee, 8 April 1988
Directive 2002/58/EC
Directive 2009/136/EC
The European Convention on Human Rights
The Charter of Fundamental Rights of the European Union
The Constitution of the United States
Working Draft Legal Instrument on Government-led Surveillance and Privacy, Version 0.7, February 28 2018, Accessed via https://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2018AnnualReportAppendix7.pdf on 15/09/18

Reports

Annual Report of the Chief Surveillance Commissioner to the Prime Minister and to Scottish Ministers for 2008-2009, Office of Surveillance Commissioners, HC 704, SG/2009/94

Annual Report of the Chief Surveillance Commissioner to the Prime Minister and to the Scottish Ministers for 2014-2015, Office of Surveillance Commissioners, HC 126, SG/2015/56

D. Anderson Q.C., *A Question of Trust, Report of Investigatory Powers Review*, (London, 2015)

D Anderson Q.C., The Terrorism Acts in 2015, *Report of the Independent Reviewer on the Operation of the Terrorism Act 2000 and Part 1 of the Terrorism Act 2006*, December 2016

European Parliament Committee on Civil Liberties, Justice and Home Affairs, *Working Document 1 on the US and EU Surveillance programmes and their impact on EU Citizens fundamental rights*, 2013

Examining Officers and Review Officers under Schedule 7 to the Terrorism Act 2000, Code of Practice, Home Office, March 2015 (last updated 17 March 2016)

House of Commons Debate, Hansard, 1 March 2011: Column 208

House of Lords Constitution Committee, 2nd Report, *Surveillance: Citizens and the State*, 2009

Intercept as Evidence, HM Government, December 2014, CM 8989

Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, D Kaye, UN Human Rights Council, 22 May 2015, A/HRC/29/32

The Data Retention and Investigatory Powers Bill, Commons Briefing Paper, House of Commons Library, 16th July 2014, Accessed via http://researchbriefings.parliament.uk/ResearchBriefing/Summary/SN06934

Publications

A Galetta, *The changing nature of the presumption of innocence in today's surveillance societies: rewrite human rights or regulate the use of surveillance technologies?*, European Journal of Law and Technology, 2013

A Home, *The Use of Intercept Evidence in Terrorism Cases*, Home Affairs Section, 24th November 2011

A M Gershowitz, *Password Protected? Can a Password Save Your Cell Phone from a Search Incident to Arrest?*, Iowa Law Review, Vol. 96:1125, 2011

Amnesty International, *Trapped in the Matrix: Secrecy, stigma, and bias in the Met's Gangs Database*, May 2018

A Stumer, *The Presumption of Innocence: Evidential and Human Rights Perspectives*, Oxford, 2010

B Emmerson et al, *Human Rights and Criminal Justice*, London, 2007

B Koops, *Commanding Decryption and the Privilege Against Self-Incrimination*, Tilburg, 2000

C Fuchs et al, *Internet and Surveillance, The Challenges of Web 2.0 and Social Media*, Routledge, 2012

C M Bradley, *The Exclusionary Rule in Germany,* Indiana University, 1983

Council of Europe, *The role of Supreme Courts in the domestic implementation of the European Convention on Human Rights*, Proceedings of the Regional Conference Belgrade, 2008

D Barnard-Wills & H Wells, *Surveillance, technology and the everyday,* Sage, 2012

D Barnard-Wills, *UK News Media Discourses of Surveillance,* The Sociological Quarterly, 2011

D J Harris et al, *Law of the European Convention on Human Rights*, 2nd Edition, New York, 2009

D P Kommers, *The Constitutional Jurisprudence of the Federal Republic of Germany,* 2nd Edition, London, 1997

D Wright & R Kreissl, *Surveillance in Europe*, London, 2015

E Lemus, *When Fingerprints Are Key: Reinstating Privacy to the Privilege against Self-Incrimination in light of Fingerprint Encryption in Smartphones,* 70 S.M.U. L Rev 533, 2017

F Davis et al, *Surveillance, Counter-Terrorism, and Comparative Constitutionalism,* London, 2014

F de Jong & L van Lent, *The Presumption of Innocence as a Counterfactual Principle,* Utrecht Law Review, 2016

F H Cate & J X Dempsey, *Bulk Collection,* Oxford, 2017

First RIPA convictions over disclosure of encryption keys, Computer Fraud & Security, Volume 2009, Issue 9, Elsevier Ltd, September 2009

G A Martin, *The Exclusionary Rule Under Foreign Law*, Journal of Criminal Law and Criminology, Volume 52 Issue 3, Article 5, 1962

G Greenwald, No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State, Toronto: McClelland & Stewart, 2014

G Orwell, *1984*, London, 1949

Harris et al, *Law of the European Convention on Human Rights*, 3rd Edition, Oxford, 2009

J D Jackson, S J Summers, *The Internationalisation of Criminal Evidence: Beyond the Common Law and Civil Law Traditions*, Cambridge, 2012

J Gesley, *Government Access to Encrypted Communications*, The Law Library of Congress, May 2016

J Lauer, *Surveillance history and the history of new media: An evidential paradigm*, Sage, 2011

J Lehmann, *Legal systems in Germany: overview*, Thomson Reuters, 2018

J Milas et al, *Unwitting subjects of surveillance and the presumption of innocence*, Computer Law & Security Review 30, 2014

J Ross, *Do Rules of Evidence Apply (Only) in the Courtroom? Deceptive Interrogation in the United States and Germany*¸ Oxford Journal of Legal Studies, Vol. 28, No. 3, 2008

J Vlahos, *The Department of Pre-Crime*, Scientific American, 2012

K Banston & R Schulman, *Deciphering the European Encryption Debate: Germany*, New America, July 11th 2017, Open Technology Institute

K D Haggerty et al, *Theorizing surveillance in crime control*, Sage, 2011

K Goldman, *Biometric Passwords and the Privilege against Self-Incrimination*, 33 Cardozo Arts & Ent. L. J. 211, 2015

K Hadjimatheou, *Surveillance: Ethical Issues, Legal Limitations, and Efficiency*, SURVEILLE, 2013

K Hadjimatheou, *Surveillance Technologies, Wrongful Criminalisation, and the Presumption of Innocence*, Springer, 2017

K Hadjimatheou, *The Relative Moral Risks of Untargeted and Targeted Surveillance*, Ethic Theory Moral Practice, 2014

Liberty, *Liberty's response to the Joint Committee on Human Rights*: "*Relaxing the Ban on the Admissibility of Intercept Evidence"*, February 2007

Liberty, *Liberty's Summary of the Investigatory Powers Bill for Second Reading in the House of Commons*, March 2016

L Woods, *The Investigatory Powers Act 2016*, European Data Protection Law Review, 2017

M Foucault, *Discipline & Punish: The Birth of the Prison*, New York, 1975

M Friedewald et al, *Surveillance, Privacy and Security*, Routledge, 2017

M Galič et al, *Bentham, Deleuze and Beyond: An Overview of Surveillance Theories from the Panopticon to Participation*, Tilburg, 2017

M Mendola, *One Step Further in the 'Surveillance Society': The Case of Predictive Policing*, Tech and Law Center, 2016

N Monaghan, *Law of Evidence*, Cambridge, 2015

N Witzleb, *Emerging Challenges in Privacy Law*, Cambridge, 2014

O Olugasa, *Rethinking Pre-Crime Surveillance versus Privacy in an Increasingly Insecure World: Imperative Expediency*, Journal of Law, Policy and Globalisation, 2017

P M. Schwartz, *Systematic government access to private-sector data in Germany*, International Data Privacy Law, 2012, Vol.2, No.4

R A Miller, *Privacy and Power*, Cambridge, 2017

R Goss, *Criminal Fair Trial Rights*, Oxford, 2014

R H Helmholz et al, *The Privilege Against Self-Incrimination*, Chicago, 1997

R L Lippke, *Taming the Presumption of Innocence*, Oxford Scholarship Online, 2016

R Reed & J Murdoch, *Human Rights Law in Scotland*, 3rd Edition, Bloomsbury, 2011

R S. Waranch, *Digital Rights Ireland Déjà vu?: Why the Bulk Acquisition Warrant Provisions of the Investigatory Powers Act 2016 are Incompatible with the Charter of Fundamental Rights of the European Union*, George Washington International Law Review, 2017

R Whitaker, *The Politics of the Right*, New York, 2015

S Ast, *The Gäfgen Judgment of the European Court of Human Rights: On the Consequences of the Threat of Torture for Criminal Proceedings*, German Law Journal Vol. 11 No. 12, 2010

S Steiger et al, *Outrage without Consequences? Post-Snowden Discourses and Governmental Practice in Germany*, Heidelberg, 2017

S Treschel, *Human Rights in Criminal Proceedings*, Oxford, 2005

T Weigend, *Assuming that the Defendant Is Not Guilty: The Presumption of Innocence in the German System of Criminal Justice*, Criminal Law and Philosophy, 2014

V Eick, *Lack of Legacy? Shadows of Surveillance after the 2006 FIFA World Cup in Germany*, Urban Studies, 2011

Online Publications

2,000 wrongly matched with possible criminals at Champions League, BBC News, 4th May 2018, Accessed via https://www.bbc.co.uk/news/uk-wales-south-west-wales-44007872 on 22/09/2018

Apple adds 'police button' to iPhones to protect users from intrusion, M Bridge, The Times, 19th August 2017, Accessed via https://www.thetimes.co.uk/article/apple-adds-police-button-to-iphones-to-protect-users-from-intrusion-5xz26bx8t on 06/02/18

Apple Announces iPhone 5s – The Most Forward Thinking Smartphone in the World, Press Release, Apple, 10th September 2013, Accessed via https://www.apple.com/newsroom/2013/09/10Apple-Announces-iPhone-5s-The-Most-Forward-Thinking-Smartphone-in-the-World on 06/02/18

Apple's Use of Face Recognition in the New iPhone: Implications, J Stanley, ACLU, 14th September 2017, Accessed via https://www.aclu.org/blog/privacy-technology/surveillance-technologies/apples-use-face-recognition-new-iphone on 07/02/18

Asian people 11 times more likely to be stopped at UK borders, analysis finds, A Travis, The Guardian, 5th December 2013, Accessed via https://www.theguardian.com/law/2013/dec/05/asian-people-stopped-uk-borders-analysis on 15/11/17

Big Brother Watch, *The Grim RIPA*, 2010, Accessed via https://www.bigbrotherwatch.org.uk/TheGrimRIPA.pdf

British woman held after being seen reading book about Syria on plane, Sian Cain, The Guardian, 4th August 2016, Accessed via https://www.theguardian.com/books/2016/aug/04/british-woman-held-after-being-seen-reading-book-about-syria-on-plane on 25/11/17

Bundesinnenministerium: "Eckpunkte der deutschen Kryptopolitik" von 1999 haben immer noch Bestand, M Monroy, Netz Politik, 17th June 2015, Accessed via https://netzpolitik.org/2015/bundesinnenministerium-eckpunkte-der-deutschen-kryptopolitik-von-1999-haben-immer-noch-bestand/ on 28/01/18

Cage director Rabbani heads for Supreme Court after appeals court rules password demands lawful, B Goodwin, Computer Weekly, 15th May 2018, Accessed via https://www.computerweekly.com/news/252441125/Cage-director-Rabbani-heads-for-Supreme-Court-after-appeals-court-rules-password-demands-lawful on 24/10/2018

Cameron announcing emergency surveillance legislation, Andrew Sparrow, The Guardian, 10th July 2014, Accessed via https://www.theguardian.com/politics/blog/2014/jul/10/cameron-announcing-emergency-surveillance-legislation-politics-live-blog on 14/08/18

Campaign group chief found guilty of refusing to divulge passwords, Owen Bowcott, The Guardian, 25th September 2017, Accessed via https://www.theguardian.com/uk-news/2017/sep/25/campaign-group-director-in-court-for-refusing-to-divulge-passwords on 30/11/17

Council spy cases hit 1,000 a month, G Rayner, The Telegraph, 12th April 2008, Accessed via https://www.telegraph.co.uk/news/uknews/1584808/Council-spy-cases-hit-1000-a-month.html on 13/08/18

D Vincent, *Surveillance, privacy and history*, History & Policy, 2013, Accessed via http://www.historyandpolicy.org/policy-papers/papers/surveillance-privacy-and-history

Edward Snowden attacks UK government over investigatory powers bill, A Gani, The Guardian, 4th November 2015, Accessed via https://www.theguardian.com/world/2015/nov/04/edward-snowden-attacks-tories-over-investigatory-powers-bill on 14/08/18

Eleanor Jones claims she was treated like a terrorist by Police Scotland, Paul Hutcheson, The Herald, 15th October 2017, Accessed via http://www.heraldscotland.com/news/15597078.Revealed__how_Police_Scotland_treated_a_political_activist_like_a_terrorist/ on 25/11/17

Fingerprint-scanning phones we have known, J Dolcourt, CNET, 12th March 2014, Accessed via https://www.cnet.com/pictures/phones-you-can-unlock-with-your-fingerprint-pictures on 06/02/18

GCHQ data collection regime violated human rights, court rules, O Bowcott, The Guardian, 13th September 2018, Accessed via https://www.theguardian.com/uk-news/2018/sep/13/gchq-data-collection-violated-human-rights-strasbourg-court-rules on 15/09/18

GCHQ intercepted foreign politicians' communications at G20 summits, E MacAskill et al, The Guardian, 17th June 2013, Accessed via https://www.theguardian.com/uk/2013/jun/16/gchq-intercepted-communications-g20-summits on 02/08/18

German federal police use Trojan virus to evade phone encryption, C Burack, DW, 27th January 2018, Accessed via https://www.dw.com/en/german-federal-police-use-trojan-virus-to-evade-phone-encryption/a-42328466 on 09/09/2018

German parliament approves controversial espionage law, J Nasr, Reuters, 21st October 2016, Accessed via https://www.reuters.com/article/us-germany-spying/german-parliament-approves-controversial-espionage-law-idUSKCN12L1ER on 08/09/2018

GFF and Amnesty are challenging strategic mass surveillance, N Markard, Freiheitsrechte, 6th November 2016, Accessed via https://freiheitsrechte.org/g10/ on 08/09/2018

Here's How Many iPhones Are Currently Being Used Worldwide, D Reisinger, Fortune, 6th March 2017, Accessed via http://fortune.com/2017/03/06/apple-iphone-use-worldwide on 06/02/18

How technology is allowing police to predict where and when crime will happen, L Dearden, The Independent, 7th October 2017, Accessed via https://www.independent.co.uk/news/uk/home-news/police-big-data-technology-predict-crime-hotspot-mapping-rusi-report-research-minority-report-a7963706.html on 22/09/2018

History of the iPhone 2007 – 2017: the journey to the iPhone X, D Grabham, T3, 10th January 2018, Accessed via https://www.t3.com/features/a-brief-history-of-the-iphone on 06/02/18

Intercept Evidence, Justice, Accessed via https://justice.org.uk/intercept-evidence/ on 27/10/2018

Met police investigating Muslim man's wrongful arrest over terrorism, Diane Taylor, The Guardian, 3rd April 2017, Accessed via https://www.theguardian.com/uk-news/2017/apr/03/met-police-investigating-muslim-man-wrongful-arrest-terrorism on 25/11/17

New surveillance law: German police allowed to hack smartphones, C Bleiker, DW, 22nd June 2017, Accessed via http://www.dw.com/en/new-surveillance-law-german-police-allowed-to-hack-smartphones/a-39372085 on 28/01/17

One surveillance camera for every 11 people in Britain, says CCTV survey, D Barrett, The Telegraph, 10th July 2013, Accessed via https://www.telegraph.co.uk/technology/10172298/One-surveillance-camera-for-every-11-people-in-Britain-says-CCTV-survey.html on 30/07/18

Revealed: British Councils used Ripa to secretly spy on public, A Asthana, The Guardian, 25th December 2016, Accessed via https://www.theguardian.com/world/2016/dec/25/british-councils-used-investigatory-powers-ripa-to-secretly-spy-on-public on 13/08/18

Richmond, Virginia, Police Department Helps Lower Crime Rates with Crime Prediction Software, C Harris, Government Technology, 21st December 2008, Accessed via http://www.govtech.com/public-safety/Richmond-Virginia-Police-Department-Helps-Lower.html on 25/10/2018

Roman Empire to the NSA: A world history of government spying, A Zurcher, BBC News, 1st November 2013, Accessed via https://www.bbc.co.uk/news/magazine-24749166 on 25/07/18

Schedule 7, Liberty, Accessed via https://www.liberty-human-rights.org.uk/human-rights/countering-terrorism/schedule-7 on 15/11/17

S Tzu, *The Art of War*, Translated by Lionel Giles, Accessed via http://classics.mit.edu/Tzu/artwar.html

Terrorism Act incompatible with human rights, court rules in David Miranda case, Owen Bowcott, The Guardian, 19th January 2016, Accessed via https://www.theguardian.com/world/2016/jan/19/terrorism-act-incompatible-with-human-rights-court-rules-in-david-miranda-case on 30/11/17

The Encryption Debate We Need, T Benner, M Hohmann, Global Public Policy Institute, 19th May 2016, Accessed via http://www.gppi.net/publications/data-technology-politics/article/the-encryption-debate-we-need/?L=0&cHash=9c0a6af9c1c08dc958640ccf396b76b6 on 28/01/18

Tracking patterns: how software claims to stop crime by analysing a burglar's behaviour, V Betz, DW, 11th December 2014, Accessed via https://www.dw.com/en/tracking-patterns-how-software-claims-to-stop-crime-by-analyzing-a-burglars-behavior/a-18109666 on 22/09/2018

UK gathering secret intelligence via covert NSA operation, N Hopkins, The Guardian, 7th June 2013, Accessed via https://www.theguardian.com/technology/2013/jun/07/uk-gathering-secret-intelligence-nsa-prism on 02/08/18

Why Minority Report was spot on, C Arthur, The Guardian, 16th June 2010, Accessed via https://www.theguardian.com/technology/2010/jun/16/minority-report-technology-comes-true on 22/09/2018

Why the Constitution Can Protect Passwords But Not Fingerprint Scans, J Linshi, TIME, 6th November 2014, Accessed via http://time.com/3558936/fingerprint-password-fifth-amendment/ on 06/02/18