Liberty v. SSHD & SSFCA: You Have the Right to Remain Silent; Anything You Say Will Be Gathered and Retained by the Government

I. OVERVIEW

The Application of National Council for Civil Liberties (Liberty) challenged the government's bulk surveillance powers in a fight for the protection of basic human rights.[1] Liberty argued that four different provisions of the Investigatory Powers Act 2019 (IPA) are incompatible with Articles 8 and 10 of the European Convention on Human Rights (ECHR).[2] Article 8 pertains to "the right to respect for private life and correspondence," and Article 10 concerns "the right to freedom of expression."[3] The four provisions concern the bulk intelligence powers, including bulk interception warrants, bulk equipment interference, warrants for bulk personal datasets, and warrants for bulk acquisition of communications data.[4] Liberty argued that the specified provisions of the IPA lack the "minimum safeguards" that have been established by the European Court of Human Rights for intelligence gathering methods, including covert surveillance.[5] Furthermore, because these provisions lack the minimum safeguards, they are not "in accordance with the law."[6] Liberty also claimed that there are insufficient safeguards for the protection of confidential journalistic material and sources, as well as insufficient safeguards for lawyer-client communications.[7] Yet the Secretary of State for the Home Department (SSHD) and the Secretary of

1. The Queen (on the application of Nat'l Council for Civil Liberties v. Sec'y of State for the Home Dep't) v. Sec'y of State for Foreign & Commonwealth Affairs (Liberty) [2019] EWHC 2057 [1], [3] (Eng.).
2. *Id.*
3. *Id.* at [3].
4. *Id.* at [2].
5. *Id.*
6. *Id.* at [3].
7. *Id.*

State for Foreign and Commonwealth Affairs (SSFCA) maintained that, while there certainly is an interference with the "right to respect for private life," there is no "meaningful" intrusion from bulk collection until the data is possibly selected for examination.[8] They argued that the legislative scheme created by the IPA was carefully constructed to be compatible with law, specifically Articles 8 and 10 of the ECHR.[9]

The High Court of Justice Queen's Bench Division gave prior judgment on a separate part of the IPA not at issue in the noted case and declared that it was incompatible with European Union law in two respects and requested that it be amended by November 1, 2018.[10] The court stayed judgment on a challenge to three other alleged incompatibilities with European Union Law pending the decision of *Privacy International v. Secretary of State for Foreign & Commonwealth Affairs* in the Court of Justice of the EU.[11] That case remains pending.[12] Following recent developments, Liberty amended its complaint and Lord Justice Singh gave permission to bring the claim for judicial review on the remaining grounds.[13] The High Court of Justice Queen's Bench Division *held* that the IPA is compatible with the HRA. *Liberty v. SSHD & SSFCA* [2019] EWHC (QB) 2057.

II. BACKGROUND

The United Kingdom (U.K.), like many other European countries today, continues to face threats to national security, including the risk of terrorist attacks and hostility from other states.[14] There have been forty-five terrorist attacks across seven European countries since 2016.[15] Extremist organizations Daesh (often called ISIS) and Al Qaeda continue to pose an international terrorist threat.[16] In the U.K. alone, a total of twelve terror plots were thwarted between March 2017 and May 2018.[17] In addition to terrorist attacks, hostile states continue to threaten the national security of the U.K. and other nations.[18] The Director General of

8. *Id.* at [6].
9. *Id.* at [8].
10. *Id.* at [11].
11. *Id.*
12. *Id.*
13. *Id.* at [13]-[14].
14. Andrew Parker, Dir. Gen., MI5, Speech at the BFV Symposium (May 14, 2018).
15. *Id.* The seven countries were the U.K., Germany, France, Belgium, Spain, Sweden, and Finland. *Id.*
16. *Id.*
17. *Id.*
18. *Id.*

MI5, Sir Andrew Parker, declared the Russian Government to be the "[c]hief protagonist among these hostile actors," emphasizing their use of technology and the Internet for media manipulation, spread of disinformation, and cyberattacks against the U.K., the United States, France, and Crimea, among others.[19] The threats of terrorism and hostility "germinate at home, abroad, and online," creating a unique global and multi-dimensional threat.[20]

In order to prevent and combat these persistent threats, the U.K., like many other countries, relies on a strong intelligence community.[21] Among the intelligence collecting methods used is the acquisition and analysis of bulk data.[22] The use of bulk data is among the few effective methods to counter the illicit use of the dark web, which is a highly encrypted space in which information is exchanged anonymously.[23] Furthermore, bulk powers allow intelligence agencies to identify and map out evolving networks leading to further gathering on likely threats and an increased ability to respond at a quick pace to increasingly diverse threats that utilize the Internet to plan attacks and radicalize supporters.[24] In fact, bulk powers have played a large part in each counterterrorism investigation over the last ten years, including seven disrupted plots.[25]

The IPA was implemented to address the interception of communications, the acquisition and retention of communications data and bulk data, and to establish the extent to which these intelligence powers can be used to interfere with privacy.[26] Bulk powers are defined as powers that allow public authorities "to have access for specified purposes to large quantities of data," a large portion of which is not related to current targets.[27] Warrants for bulk data are not generally available to public authorities and must be applied for by the head of an intelligence organization and issued only by the Secretary of State.[28] Bulk warrants include bulk interception warrants, bulk equipment interference warrants, bulk acquisition warrants, and bulk personal datasets.[29]

---

19. *Id.*
20. *Id.*
21. *Id.*
22. DAVID ANDERSON, INDEP. REVIEWER OF TERRORISM LEGISLATION, REPORT OF THE BULK POWERS REVIEW 1 (2016).
23. *See id.* at 152.
24. *See id.*
25. *Id.* at 146.
26. Investigatory Powers Act 2016, c. 25, § 1 (Eng.).
27. ANDERSON, *supra* note 22, at 2.
28. Investigatory Powers Act §§ 18, 138, 141, 158, 160, 178, 182.
29. *Id.* §§ 101, 136, 176; *see also* ANDERSON, *supra* note 22, at 4.

The passage of the IPA was not without oversight or pre-legislative scrutiny.[30] During its passage through Parliament, the IPA endured scrutiny by three committees: the House of Commons Science and Technology, the Intelligence and Security Committee of Parliament, and the Joint Committee on the Bill.[31] Each committee reported their recommendations, which were then reflected in a new version of the IPA.[32] The IPA was further reviewed by the House of Commons Public Bill Committee, the Joint Committee on Human Rights, the House of Lords Constitution Committee, and the House of Lords Delegated Powers and Regulatory Reform Committee prior to its passage.[33]

The IPA itself contains various safeguards.[34] The IPA contains a "double-lock" feature for warrants that authorize the use of intrusive powers.[35] This requires that an independent Judicial Commissioner must approve the decision of the Secretary of State before a warrant is authorized.[36] First, the Secretary of State must decide whether the warrant is necessary in the interest of national security.[37] The Secretary must also be satisfied that the authorized conduct is proportionate to the result sought.[38] Each warrant must specify an operational purpose, which must be taken from a specified list approved by the Secretary of State, reviewed every three months by the Parliamentary Intelligence and Security Committee, and reviewed yearly by the Prime Minister.[39] The Secretary of State also must ensure that safeguards ensure that the selection of data for examination, particularly communications data, is necessary and proportionate and carried out only for the operational purposes specified in the warrant.[40] A Judicial Commissioner must then approve the decisions of the Secretary of State by applying the principles of judicial review.[41]

The IPA also creates a new regulatory and supervisory body, which is headed by the Investigatory Powers Commissioner (IPC).[42] Additionally,

---

30. ANDERSON, *supra* note 22, at 9.
31. *Id.*
32. *Id.*
33. *Id.*
34. Investigatory Powers Act 2016, c. 25, §§ 111-14, 129-31, 150-55, 171-73, 191-96, 221-24 (Eng.).
35. *Id.* §§ 108, 140, 159, 179, 208.
36. *Id.*
37. *Id.* § 138.
38. *Id.*
39. *Id.* §§ 142, 161,183.
40. *Id.*
41. *Id.* §§ 23, 140, 159, 179.
42. ANDERSON, *supra* note 22 at 47-48. The IPC must be an individual who holds or has held high judicial office. *Id.*

the main purpose of bulk interception and equipment interference warrants must be to obtain overseas-related communications.[43] The selection for examination of protected material[44] is subject to the British Islands safeguard, meaning that the content cannot be selected if any criteria used for its selection is "referable to an individual known to be in the British Islands at the time" and the reason for using the "criteria is to identify the content of communications sent by, or intended for, that individual."[45] Specific provisions of the IPA also address additional safeguards for legal privilege and confidential journalistic material, in addition to general duties for privacy.[46] Additionally, codes of practice have been made under the IPA to protect the public interest in items subject to legal privilege and confidential journalistic material.[47]

The Human Rights Act of 1998 (HRA) incorporates the ECHR into U.K. law.[48] Section 6(1) of the HRA makes it "unlawful for a public authority to act in a way which is incompatible with a Convention right."[49] Thus, as public authorities, the Secretary of State, intelligence agencies, and the police must act in a way that is compatible with Convention rights, with the exception that they could not have acted differently as a result of a provision of primary legislation.[50] Additionally, section 3(1) of the HRA requires that, to the extent it is possible, primary legislation "must be read and given effect in a way which is compatible with the Convention rights."[51] When primary legislation cannot be read and given effect in such a way, section 4 of the HRA becomes relevant.[52] Section 4 provides that if a relevant court, namely the High Court for London and Wales, determines that the legislation is incompatible with a Convention right, then it may make a declaration that it is incompatible."[53] This determination doesn't affect the validity or continuing operation of the legislation, nor is it binding on the parties to the case in which the determination is made, but

43. Investigatory Powers Act § 9. Overseas-related communications are communications that are sent to or received by persons outside of the British Islands or overseas-related equipment data. *Id.*

44. Protected material is defined as content, which is not equipment data or not private information.

45. Investigatory Powers Act § 152.

46. *Id.* §§ 153, 194, 222-23.

47. *Id.* § 241.

48. Bonnie H. Weinstein, *The UK Human Rights Act*, ASIL INSIGHTS (May 18, 2001), https://www.asil.org/insights/volume/6/issue/12/uk-human-rights-act.

49. Human Rights Act 1998, c. 42, § 6.

50. *Id.*

51. *Id.* § 3.

52. *Id.* § 4.

53. *Id.*

rather, it enables the Minister of the Crown to make a remedial order, which enables the government to amend the legislation as required.[54]

The relevant sections of the HRA are article 8 and article 10.[55] Article 8 solidifies the "right to respect for his private and family life, his home and his correspondence" and makes it clear that there should be no interference with this right by a public authority unless it is "in accordance with the law and is necessary in a democratic society."[56] Article 10 provides for the "right to freedom of expression."[57] Article 10 contains a similar provision to Article 8 and emphasizes that there should only be restrictions as "prescribed by law and are necessary in a democratic society."[58]

Thus, any interference with the rights in articles 8 and 10 must be in accordance with the law.[59] The relevant case law of the European Court of Human Rights has specified that this requirement is made up of three elements.[60] The elements are as follows: (1) the interference has to be authorized by domestic law; (2) the domestic law must be of a certain quality, mainly it has to be accessible; and (3) the quality of law requires that it must be reasonably foreseeable.[61] In *Weber & Saravia v. Germany*, the court summarized the third element.[62] The court emphasized that foreseeability does not mean that a citizen should be able to foresee when his or her communications are likely to be intercepted by the authorities, but rather that domestic law should be clear as to give adequate indication of the circumstances in which authorities are authorized to use these measures.[63]

Articles 8 and 10 must also be necessary in a democratic society.[64] Here, the court must balance the interest of the state in protecting its national security against the severity of the interference in the citizen's right to privacy.[65] Courts have consistently recognized that public authorities have a "fairly wide" margin for choosing the means to reach the legitimate objective of protecting national security, but the court must

54. *Id*
55. *Id.* sch. 1.
56. *Id.*
57. *Id.*
58. *Id.*
59. *See id.*
60. *See* Weber & Saravia v. Germany, 46 Eur. Ct. H.R. 19, 21 (2008).
61. *See id.*
62. *Id.* ¶¶ 93-94.
63. *Id.* ¶ 93.
64. *See id.* ¶ 106.
65. *Id.*

also be satisfied that there are "adequate and effective guarantees against abuse."[66] In making such an assessment, the court will consider all the circumstances of the case, particularly the following factors: "the nature, scope, and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorize, carry out and supervise them, and the kind of remedy provided by national law."[67] Furthermore, in *Zakharov v. Russia*, the Grand Chamber of the European Court of Human Rights noted that the values of democratic society need to be followed as closely as possible through the review and supervision of surveillance measures.[68] The court in *Zakharov* also emphasized that there are three stages at which review and supervision come in, those being "when the surveillance is first ordered, while it is being carried out, [and] after it has been terminated."[69]

The Supreme Court of the United Kingdom also provides substantial guidance on the requirements that an interference must be "in accordance with the law" and "necessary in a democratic society."[70] In *R(P) v. Secretary of State for Justice*, the Supreme Court noted that an interference with Convention rights cannot be in accordance with law unless there are sufficient safeguards that are exercised on known legal principles such that it makes its application reasonably foreseeable.[71] The Supreme Court stated that if a measure authorizes an exercise of power that is not constrained by law, then it is not in accordance with law.[72] Yet there are some instances where the argument for incompatibility of primary legislation is that the legislation is not compatible with Convention rights.[73] In this situation, it is about the legislation itself, not the application of the legislation to the facts of the particular case.[74]

It is important to note that an independent tribunal, the Investigatory Powers Tribunal, was created under the Regulation of Investigatory Powers Act 2000 (RIPA) and strengthened by the IPA to hear claims by citizens who believe they have been victims of wrongful interference by covert investigative techniques, including bulk surveillance.[75] The

66. *See id.*; *see also* Silver v. United Kingdom, 5 Eur. Ct. H.R. 347 (1983).
67. *Weber & Saravia*, 46 Eur. Ct. H.R. ¶ 106.
68. Zakharov v. Russia, 63 Eur. Ct. H.R. 17, ¶ 233 (2016).
69. *Id.*
70. *See* R(P) v. Sec'y of State for Justice [2019] UKSC 3, [2019] 2 WLR 509.
71. *Id.*¶ 31.
72. *Id.*¶ 17.
73. *See* R(H) v. Mental Health Review Tribunal for N. & E. London Region [2001] EWCA (Civ.) 415, [2002] QB 1.
74. *See id.*
75. INVESTIGATORY POWERS TRIBUNAL, https://www.ipt-uk.com/default.asp (2016).

Tribunal does not require complainants to provide evidence to support their claim, but rather they must specify the activity that has taken place.[76] The Tribunal then investigates and determines the validity of the complaints and makes the relevant orders to remedy the interference.[77]

The recent case, *Big Brother Watch & Ors v. United Kingdom*, in the European Court of Human Rights, addressed similar complaints to those at issue in the noted case.[78] In that case, the complaints regarded the compatibility of article 8 of the HRA with two sections of the RIPA that addressed bulk interception of communications and acquisition of communications data.[79] The court applied the various tests from *Weber & Saravia* and *Zakharov* and found that the various safeguards in RIPA created an acceptable balance between national security and human rights in most cases.[80] The court found the safeguards insufficient for selection of bearers or cables for bulk interception and the identification of selectors and search criteria.[81] Yet the court failed to set out what would make them sufficient, other than that robust independent oversight is necessary.[82]

III. THE COURT'S DECISION

In the noted case, the High Court of Justice Queen's Bench Division relied on the tests supplied by *Weber & Saravia* and *Zakharov* to analyze the balance between national security and human rights to determine the compatibility of the relevant provisions of the IPA with HRA in accordance with precedent.[83] The court held that overall the IPA is compatible with the HRA.[84] At the outset, the court emphasized that the issue here is not whether the actual practices or activity are incompatible with articles 8 and 10, but whether the legislation, the IPA, is incompatible.[85] The court looked at each warrant separately but analyzed their compatibility similarly.[86] The court first noted the critical role that bulk powers play in national security and the protection of the public.[87]

---

76. *Id.*
77. *Id.*
78. *See* Big Brother Watch & Ors v. United Kingdom, Eur. Ct. H.R. 3 (2018), https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-186048%22]}.
79. *Id.*
80. *Id.* ¶ 320.
81. *Id.* ¶ 347.
82. *See id.*
83. *See* Liberty [2019] EWHC 2057 [1], [3] (Eng.).
84. *Id.* at [399].
85. *Id.* at [174], [224].
86. *See generally id.*
87. *Id.* at [158]-[159].

The court then found that in regard to the regime for bulk interception warrants, bulk and thematic equipment interference warrants, bulk personal datasets, and bulk acquisition warrants, the IPA is compatible with the Convention rights because the Act contains interlocking safeguards that are sufficient to meet the Convention requirements of quality of law.[88] Next, the court acknowledged that it is not possible to apply the findings from the *Big Brother Watch* to the new statutory scheme of the IPA because of the added safeguards.[89] Finally, the court found that the added safeguards are sufficient to "prevent the risk of abuse of discretionary power" and "arbitrary interference," and thus those sections of the IPA are compatible with Convention rights.[90] The court then looked specifically at lawyer-client communications and confidential journalistic material and ultimately found that the added safeguards were sufficient.[91]

When determining the compatibility of the regime for bulk interception warrants, bulk and thematic equipment interference warrants, bulk personal datasets, and bulk acquisition warrants, the court first noted the critical role that bulk powers play in national security and the protection of the public.[92] The court referred to the Bulk Powers Review in which Lord Anderson emphasized that bulk interception and equipment interference have shown to be of "vital utility" and alternatives have fallen short in terms of speed of acquisition, cost, intrusiveness, and risk to life.[93] Lord Anderson also emphasized the utility of bulk personal datasets (BPDs), noting that they enable the identification of targets and enhance the ability to quickly counter threats.[94] The court noted that the reason for the utility of bulk powers is that in the early stages of an investigation, it may not be possible to know who will turn out to be subjects of interest.[95] Furthermore, bulk acquisition warrants for communications data are particularly crucial to counterterrorism and counter-espionage in terms of providing fast target identification for dealing with imminent threats and disrupting terrorist operations.[96] The main advantage of the bulk powers

88. *Id.* at [178], [240], [264].
89. *Id.* at [161].
90. *Id.* at [208], [240.3].
91. *Id.* at [292], [352].
92. *Id.* at [158]-[159].
93. ANDERSON, *supra* note 22, at 91.
94. *Id.* at 42.
95. *Liberty* [2019] EWHC 2057 at [158].
96. ANDERSON, *supra* note 22, at 92.

that the court emphasized was the ability to obtain accurate information faster and less intrusively than alternatives.[97]

The court then emphasized that the issue of compatibility with the Convention must be determined with deference to the sum of the interlocking safeguards available at each stage of the interception process.[98] It stressed that in particular the analysis should not be done with reference to the potential range of information that could possibly be retained through bulk interception.[99] Many of the same safeguards apply to each type of warrant.[100] The court emphasized the importance of the British Islands safeguard, the "double-lock" feature, and the IPT.[101]

Next, the court acknowledged that it is not possible to apply the findings from the *Big Brother Watch* to the new statutory scheme of the IPA.[102] This is due to the introduction of the office of the IPC created by the IPA and the new "double-lock" feature that necessitates approval by a Judicial Commissioner at the warrant stage prior to even being able to obtain bulk data.[103] For example, specifically for BPD warrants, the court concluded that the double-lock was a sufficient safeguard because if, on a particular set of facts, it is not necessary or proportionate to issue a class BPD warrant[104] because it would be less intrusive to issue a specific warrant, then the Secretary of State will not be able to issue the warrant, nor would a Judicial Commissioner approve it.[105] The safeguards contained in the IPA did not previously apply to the Telecommunications Act 1986 or RIPA.[106]

The court further distinguished that there will be an increased ability to regulate the selection of bearers[107] under the IPA because the warrant applications must contain descriptions of which communications are to be intercepted and the selection of bearers is subject to the Interception Code of Practice, which necessitates that their selection should be based on those most likely to contain overseas-related communications.[108] Furthermore, the requirement that bulk interception and equipment warrants have to

97. *Liberty* [2019] EWHC 2057 at [222]; *see also* ANDERSON, *supra* note 22.
98. *Liberty* [2019] EWHC 2057 at [160].
99. *Id.*
100. *Id.* at [182]; Investigatory Powers Act 2016, c. 25, § 193.
101. *Liberty* [2019] EWHC 2057 at [182]; Investigatory Powers Act 2016, c. 25, § 193.
102. *Liberty* [2019] EWHC 2057 at [161].
103. *Id.*
104. *Id.* (class refers to bulk collection).
105. *Id.* at [225].
106. *Id.*
107. *Id.* Bearers allow the transmission of information signals between network interfaces.
108. *Id.* at [162]-[163]; Investigatory Powers Act § 142.

specify any operational purposes for which the data obtained may be selected for examination acts as a safeguard not only for the selection of bearers, but for search criteria for examination as well.[109] The court emphasized that the method in which the list of operational purposes must be approved creates a significant amount of oversight and accountability.[110]

Next, the court stressed that the IPA has narrowed the definition of "overseas-related communication."[111] The new definition now excludes Google searches by individuals within the British Islands.[112] In its decision, the court particularly stressed that the "British Islands Safeguard" requires that the Secretary of State ensure that the selection of protected material and intercepted content for examination must meet selection conditions.[113] The court rejected the claims that the absence of a British Islands Safeguard for nonprotected material, secondary data, and the examination of BPDs make those sections of the IPA incompatible because of the other inter-locking safeguards contained in the IPA that prevent the abuse of power.[114] Furthermore, the court emphasized that although the British Islands safeguard does not protect them, they are still subject to safeguards relating to the issuing of a warrant, IPC oversight, the necessity and proportionality tests, the operational purposes test, and JC Approval.[115]

The court also made sure to emphasize in its analysis of the statutory scheme of the IPA that, under the HRA, a person is able to bring a claim to the IPT.[116] Thus, an independent tribunal can determine the issue of whether the HRA has been breached on the facts of a particular case.[117] Furthermore, the IPT has the ability to review acts of the office of the IPC, creating another level of accountability.[118]

After analyzing the compatibility of the regime for bulk interception warrants and the compatibility of each type of warrant, the court looked specifically at lawyer-client communications and confidential journalistic material.[119] In its analysis, the court looked at the various safeguards and

---

109. *Liberty* [2019] EWHC 2057 at [166]-[167]; Investigatory Powers Act § 142.
110. *Liberty* [2019] EWHC 2057 at [167].
111. *Id.* at [164].
112. *Id.*
113. *Id.* at [181]; Investigatory Powers Act § 193.
114. *Liberty* [2019] EWHC 2057 at [181], [256]; Investigatory Powers Act 2016, §§ 193, 203.
115. *Liberty* [2019] EWHC 2057 at [256].
116. *Id.* at [170].
117. *Id.*
118. *Id.* at [196].
119. *Id.* at [271].

how they apply to both types of communications and material.[120] The court noted that a wide range of "dedicated and detailed" safeguards tailored for legally privileged information and confidential journalistic material are included in the IPA.[121] The court ultimately concluded that the rules regarding legally privileged items set out in the IPA contain sufficient safeguards as to avoid arbitrary interference.[122]

IV. ANALYSIS

In a post-Edward Snowden world, the average citizen is increasingly aware, and wary, of the extent of government surveillance, especially in regard to invasions of privacy.[123] At the same time, we also live in a post-9/11 world in which terrorism is a critical and very real issue.[124] Snowden's publications lead to an onslaught of litigation to determine the legality of surveillance practices and the extent of interference permitted by basic human rights.[125] At the same time, an increase in threats and extremist groups has led to an increased need for effective national security and counterterrorism measures.[126] Thus, one of the most important debates that has emerged is about the balance between national security interests and privacy.[127]

It is interesting and imperative to note that the first step of inquiry by the court for each challenged section of the IPA was the critical role that bulk powers play in intelligence gathering and national security.[128] It must be opined whether the court's decision was influenced due to the potential national security ramifications of the decision.[129] One could argue that the government has every incentive to err on the side of caution when it comes to national security because the general public would be much less forgiving if another terrorist attack were to occur.[130] On the other hand, despite the looming threat of terrorism, more people are killed annually due to natural disasters than terrorist attacks.[131] Although national security

120. *Id.* at [273]-[281].
121. *Id.*
122. *Id.*
123. MARY ARDEN, HUMAN RIGHTS AND EUROPEAN LAW: BUILDING NEW LEGAL ORDERS 148 (2015).
124. *Id.*
125. *Id.*
126. *Id.*
127. *Id.* at 201.
128. Liberty [2019] EWHC 2057 at [158]-[159] (Eng.).
129. *Id.*
130. *Id.*
131. *Id.*

and counterterrorism are of grave importance, the court should be careful to keep the actual threat in perspective when it comes to the liberty of citizens.[132]

That being said, the judiciary must be careful to truly balance the needs between national security and human rights.[133] There is a fine line between too much intrusion and not enough, leading to lackluster intelligence gathering that could potentially lead to a national security disaster.[134] On the flip side of that, despite the best intelligence efforts, there will always remain a risk of terrorism.[135] Nothing will make citizens and countries completely invulnerable to terrorism and no amount of intrusion will change that.[136] Individual liberties can only be restricted so far in the name of national security and making people feel safe; at some point, the result is the loss of the very rights that make up a free and democratic society.[137] The courts must keep these considerations in mind when deciding whether there truly is a balance between national security and human rights.[138]

In the noted case, the court predominantly focused on the importance of bulk intelligence collection and the safeguards that prevent the intelligence services from going too far.[139] The court seemed to spend an insignificant amount of time exploring the reality and extent of privacy intrusions.[140] The decision of the court felt one-sided, looking in from a government's perspective on the importance of bulk intelligence collection and ignoring the actual effects that this interference can have on individuals.[141]

The implications of the decision in the noted case are two-fold.[142] On one hand, the decision results in a decreased ability of the public to challenge the intelligence practices of the government, especially in terms of human rights violations, as well as challenges to the IPA.[143] While individuals still have the opportunity to bring a claim to the IPT, the

132. *Id.*
133. *Id.*
134. *Id.*
135. *Id.*
136. *Id.*
137. *Id.*
138. *See id.* at [174], [178].
139. *See id.*
140. *See id.*
141. *See id.*
142. *See id.*; INVESTIGATORY POWERS TRIBUNAL, *supra* note 75.
143. *See Liberty* [2019] EWHC 2057.

remedies of the Tribunal are extremely limited.[144] On the other hand, the decision results in a win for the intelligence community in terms of bulk data collection and the ongoing debates about its legality and human rights implications.[145] In terms of national security and intelligence gathering initiatives, this case demonstrates a push towards acceptance of controversial intelligence practices and acknowledgement that these bulk collection efforts fall under the permissibility of the HRA.[146]

V. CONCLUSION

The High Court of Justice Queen's Bench Division relied on the tests established by the European Court of Human Rights and the Supreme Court of the United Kingdom to provide a basis to analyze the balance between national security and human rights in order to determine the compatibility of the relevant provisions of the IPA with the HRA.[147] The court followed precedent, but throughout its analysis, it erred on the side of caution and decided the case with the threat of terrorist attacks, hostile actors, and national security weighing heavily on its mind. The lack of focus on the fundamental rights at risk of being encroached upon resulted in a balancing test that simply lacked balance and a future in which national security is seemingly more valuable than individual liberties.

India Trummer*

144. INVESTIGATORY POWERS TRIBUNAL, *supra* note 75.
145. *See Liberty* [2019] EWHC 2057.
146. *See id.*
147. *See id.*

* © 2020 India Trummer. J.D. candidate 2021, Tulane University Law School; B.A. 2018, University of Mississippi. I would like to thank the members of the *Tulane Journal of International and Comparative Law* for their guidance and help preparing this piece for publication. I would also like to thank my family and friends for their continued support and encouragement throughout the years as I've pursued my academic and professional goals.