STUDIES IN LAW, POLITICS,
AND SOCIETY

STUDIES IN LAW, POLITICS, AND SOCIETY

Series Editor: Austin Sarat

Recent volumes:

Volumes 1–2:	Edited by Rita J. Simon
Volume 3:	Edited by Steven Spitzer
Volumes 4–9:	Edited by Steven Spitzer and Andrew S. Scull
Volumes 10–16:	Edited by Susan S. Sibey and Austin Sarat
Volumes 17–33:	Edited by Austin Sarat and Patricia Ewick
Volumes 34–77:	Edited by Austin Sarat
Volume 78:	Edited by Livia Holden and Austin Sarat
Volume 79:	Edited by Austin Sarat
Volume 80:	Edited by Austin Sarat
Volume 81:	Edited by Austin Sarat

STUDIES IN LAW, POLITICS, AND SOCIETY VOLUME 82

STUDIES IN LAW, POLITICS, AND SOCIETY

EDITED BY

AUSTIN SARAT
Amherst College, USA

United Kingdom – North America – Japan
India – Malaysia – China

Emerald Publishing Limited
Howard House, Wagon Lane, Bingley BD16 1WA, UK

First edition 2020

British Library Cataloguing in Publication Data
A catalogue record for this book is available from the British Library

ISBN: 978-1-83982-279-7 (Print)
ISBN: 978-1-83982-278-0 (Online)
ISBN: 978-1-83982-280-3 (Epub)

ISSN: 1059-4337 (Series)

CONTENTS

This page intentionally left blank

LIST OF CONTRIBUTORS

Christos Boukalas	Northumbria University, UK
Elizabeth Brown	San Francisco State University, USA
Matthew C. Canfield	Drake University, USA
Chris Kendall	University of Puget Sound, USA
Verónica Michel	John Jay College – CUNY, USA
Jesse J. Norris	State University of New York at Fredonia, USA
Amy Smith	San Francisco State University, USA

This page intentionally left blank

EDITORIAL BOARD

This page intentionally left blank

CHAPTER 1

OVERCOMING LIBERAL DEMOCRACY: "THREAT GOVERNMENTALITY" AND THE EMPOWERMENT OF INTELLIGENCE IN THE UK INVESTIGATORY POWERS ACT

Christos Boukalas

ABSTRACT

The sudden rise of the socio-political importance of security that has marked the twenty-first century entails a commensurate empowerment of the intelligence apparatus. This chapter takes the Investigatory Powers Act 2016 as a vantage point from where to address the political significance of this development. It provides an account of the powers the Act grants intelligence agencies, concluding that it effectively legalizes their operational paradigm. Further, the socio-legal dynamics that informed the Act lead the chapter to conclude that Intelligence has become a dominant apparatus within the state. This chapter pivots at this point. It seeks to identify, first, the reasons of this empowerment; and, second, its effects on liberal-democratic forms, including the rule of law. The key reason for intelligence empowerment is the adoption of a pre-emptive security strategy, geared toward neutralizing threats that are yet unformed. Regarding its effects on liberal democracy, the chapter notes the incompatibility of the logic of intelligence with the rule of law. It further argues that the empowerment of intelligence pertains to the rise of a new threat-based governmental logic. It outlines the core premises of this logic to argue that they strengthen the anti-democratic elements in liberalism, but in a manner that liberalism is overcome.

Studies in Law, Politics, and Society, Volume 82, 1–25

ISSN: 1059-4337/doi:10.1108/S1059-433720200000082002

Keywords: Biopolitics; electronic surveillance; Investigatory Powers Act; liberal democracy; pre-emption; rule of law; threat governmentality; total intelligence

INTRODUCTION

The Investigatory Powers Act 2016 (IPA) regulates the state's electronic surveillance powers. It was created in a period marked, on the one hand, by the need to combat security threats; and, on the other hand, by the exposure of systematic mass infringements on privacy by the security apparatus. It has, therefore, been the subject of intense controversy among legal, political, and civil society actors. While it was meant to clarify and settle electronic surveillance powers, it is itself unsettled, as a High Court decision forced the government to reconsider some of its key provisions.[1] The legal uncertainty arising from the Act, its unstable architecture (McKay, 2017, pp. 24–25) and the persistent conflict about the powers it provides are symptomatic of a tension between two core political values. On the one hand, security is the *sine qua non* of statehood, the "supreme concept" of the state, including the liberal-capitalist state (Neocleous, 2000, p. 61, Neocleous, 2008). On the other hand, privacy, and the division of social life into distinct public and private spheres that it implies, is an essential feature of the liberal state and specifies it as liberal. Thus, the opposition between security and privacy is, ultimately, one between the preservation of the liberal *state* and the preservation of the state *as liberal*. The IPA causes concern in segments of civil society and frictions within the state precisely because it is a law that touches on the character of political organization.

Accordingly, this chapter moves beyond a conceptualization of the IPA in terms of rights, to outline its deeper implications for the form of the state, for liberal democracy. It treats IPA as a legal and (therefore) political datum, and unfolds its meaning with regard to the "logic" of the state, that is, the ontological and epistemological premises that inform governmental practice and help it cohere. To unwrap the implications of the IPA for liberal democracy, the chapter outlines the character of security and the associated governmental logic, and assesses them from a liberal and a democratic viewpoint. Starting from an account of the IPA and the socio-legal dynamics that inform it, the chapter establishes that the IPA represents an institutional empowerment of Intelligence[2] and attributes it to the rise of a pre-emptive modality in the exercise of state power. On this basis, the chapter assesses the significance of Intelligence empowerment with regard to the rule of law and, more broadly, to liberal democracy. It argues that the empowerment of Intelligence is part of a nascent governmental logic that departs from both liberal and democratic politics. On this basis, it questions whether the defence of privacy rights is an adequate form of resistance (e.g., Amnesty International, 2016; Liberty, 2015; Privacy International, 2015. For a critical review of this approach: Goodman, 2018, pp. 6–9).

Specifically, the first substantive section outlines the key provisions of the IPA and the socio-legal dynamics that informed it – especially the clash between Intelligence demands and judicial decisions. It claims that IPA legislates "total intelligence," that is, the perpetual monitoring of all individuals in all their transactions. It also argues that the vindication of Intelligence interests in the face of social and judicial opposition signals an empowerment of Intelligence. The second section identifies other expressions of this empowerment in the resources allocated to Intelligence, its relation to law enforcement, and the insertion of its operational logic into criminal law. It concludes that Intelligence has become a dominant state apparatus and that a key target of its surveillance is political activity and association. This is a consequence of a pre-emptive approach to security, based on the perception of social potentiality as pregnant with a threat – a threat that consists of the adoption and enactment of non-liberal politics. The third and fourth sections trace the implications of the empowerment of Intelligence for the juridico-political constellation. The third section finds that the logic of Intelligence is incompatible with the rule of law and argues that the IPA attempts to reframe the latter so that it can accommodate the former. The final substantive section examines the implications of Intelligence empowerment for liberalism and for democratic politics, the two political projects that comprise liberal democracy. It argues that the empowerment of Intelligence pertains to a novel governmental logic that is based on the ontological assumption of an omnipresent but unknowable threat and aims to pre-emptively neutralize it. This "threat governmentality" is a departure from a liberal biopolitical logic toward a post-liberal, onto-political one. This transition strengthens the core anti-democratic element of liberalism, the premise that political functions should be undertaken by political experts. Yet, by founding governmental expertise on a basis of unknowability and irrationality, it also undermines and transcends liberalism.

INVESTIGATORY POWERS ACT

Despite its political significance and its controversial reception in civil society, the IPA has been largely ignored by (socio-) legal scholarship.[3] In this section, the chapter seeks to rectify this perplexing omission. It outlines the main contours of the Act, as well as the key social and legal dynamics involved in its creation.

The IPA sets up a comprehensive regulatory framework for electronic surveillance. It upgrades the previous regulatory regime, which had been perforated by judicial decisions and technological developments (Anderson, 2015, p. 4). This upgrade occurred in a conflictual context, outlined, on one hand, by counterterrorism exigencies and, on the other, by social concerns and legal challenges triggered by the Snowden disclosure of the scale and scope of electronic surveillance by British and American Intelligence (Lyon, 2015, pp. 15–42; Snowden, n.d.). The Act regulates communications' data collection, interception of communications, interference with electronic equipment, and the bulk employment of these techniques. While consolidating and expanding surveillance powers, the IPA also subjects them to judicial control.

Oversight

The Act maintains the high-level executive authorization that was already required for most surveillance methods. It couples it with a requirement for judicial approval, thus bringing surveillance under a "double lock." It introduces the Office of the Investigatory Powers Commissioner (IPC) comprised of senior judges acting as Judicial Commissioners. They are appointed by the Prime Minister and serve renewable three-year terms (ss. 227–228).

The Commissioners overview electronic surveillance practices (s. 229) that cannot lawfully proceed without their approval. Indeed, most IPA clauses are dedicated to outlining the authorization process and requirements for each surveillance method. The IPC reports yearly to the Prime Minister on the Commissioners' reviewing activity, and may make relevant recommendations. The Prime Minister must publish the IPC report, but can redact parts thereof at her discretion (s. 234). Judicial overview encompasses interception of electronic communications, interference with electronic equipment and bulk surveillance. It does not cover the surveillance of communications' data. Below, I examine the surveillance methods the IPA addresses, the associated judicial controls, and the related social and legal dynamics.

Communications Data Surveillance

Communications data (CD) is the data ensuing from a transaction's occurrence. They comprise personal details (name, address, e-mail address, telephone number, bank account details, etc.) of the persons engaged; the apparatus, location, and time of a transmission; the websites visited, and the programs, applications, and files used in the course of a communication (s. 261(5)) (Anderson, 2015, p. 96; McKay, 2017, pp. 20–23). Moreover, the IPA explicitly classifies weblogs (Internet Connection Records; ss. 61–62, s. 85) as CD. Weblogs are self-generating records of internet activity that identify the websites, applications, messaging services (etc.) to which a device has been connected.

Access to CD is available to virtually all public sector bodies. Listed in Schedule 4 are over 60 authorities, ranging from the Metropolitan Police to the Welsh Ambulance Service, that have direct access. All other public authorities can gain access through collaboration with listed ones (s. 74, ss. 78–80). The grounds on which this type of surveillance can occur are broad and open-ended, encompassing, *inter alia*, national security, identification of dead people, investigating benefit fraud, and "exercising functions relating to financial security" (s. 46(7); McKay, 2017, p. 83). Surveillance is authorized by an agent in a listed authority when she appreciates that it is necessary and proportionate for the purposes of the investigation (s. 61).

As CD is stored by Communications Service Providers (CSPs), the IPA imposes on them a duty to comply with relevant investigation requests (s. 66), and penalizes disclosure of the fact that a request has been issued (s. 82). Moreover, the Home Secretary, with the approval of a Judicial Commissioner, can request that CSPs retain CD for a year-long period (s. 87 & 89).

The surveillance of CD had been contested in three of its aspects: its definition (what is classified as CD); its nature (whether it is personal information or not); and the length of data retention. In 2014, the European Court of Justice (ECJ)

dealt a decisive blow to the retention regime of EU member states, by invalidating the EU Retention Data Directive (2006/24/EC) that allowed a 12-month long data retention.[4] The UK reacted by issuing the Data Retention and Investigatory Powers Act 2014 (DRIPA) that authorized 12-month retention and was scheduled to expire by the end of 2016 (Anderson, 2015, pp. 15–16, 32, 86–91). In July 2015, the High Court declared DRIPA data retention powers incompatible with EU law,[5] for they were not limited to serious offences and did not provide for judicial supervision. In 2016, the ECJ (Grand Chamber) found them excessive, unnecessary, and declared them unjustifiable in a democratic society.[6] By contrast, police and Intelligence demanded the maintenance of long retention periods (Anderson, 2015, p. 167, 193, 197; Travis, 2015). The IPA installs precisely the judicial controls the High Court found lacking. Yet, it does so in order to entrench the regime of expanded retention. This contradicts the ECJ decision but vindicates the positions of Intelligence.

With regard to the definition of CD, Intelligence demanded that it includes weblogs. Lack of explicit reference to weblogs would qualify them by default as content and raise the authorization threshold for their surveillance. Again, the government satisfied Intelligence's requests. This makes the UK the only western jurisdiction that classifies weblogs as CD, thus allowing its agencies to reconstruct potentially personal and detailed web-browsing profiles on the basis of self-issued authorizations (Anderson, 2015, pp. 176–179, 197; Privacy International, 2015, p. 6).

The inclusion of weblogs expands the remit of CD surveillance, that is, of the only method exempt from regulation. Its exemption is premised on the government's persistent refusal to acknowledge CD as personal and private information. This discards claims raised by civil society groups (Liberty, Open Rights Group; Guardian), by the parliamentary Intelligence and Security Committee, and by the ECJ that the volume of CD, its richness, the inherently hybrid (content + data) nature of internet communications and the capacity of state authorities to combine and analyse multiple types of CD from multiple sources, can make CD surveillance highly intrusive and its distinction from content interception problematic (Anderson, 2015, pp. 78–79, 221–222, 2016; Goodman, 2018, pp. 7–8; International Commission of Jurists, 2014; McKay, 2017, p. 13). By contrast, the MI5 Chief, in a 2015 correspondence with the Home Secretary, protested that, given the sheer volume of CD surveillance,[7] any attempt to regulate it would render the practice unworkable (Weaver, 2016). Again, the IPA vindicates Intelligence positions in the face of social and judicial concerns and inscribes Intelligence requests in legislation.

This single-mindedness has brought the first judicial blow to the IPA. In April 2018 the High Court found that provisions on access to retained CD contravene fundamental rights in EU law, as they are not limited to combating serious crime and do not require independent authorization for access to retained data.[8] Accordingly, the government is considering introducing a new administrative body to dispatch relevant authorizations, and to limit retention and acquisition of collected data to "serious crime" purposes. It defines "serious crime" as offences with a maximum sentence of more than six months and, ironically, as "any offence involving the sending of a communication or a breach of privacy" (Smith, 2016).

Interception and the Authorization Process

Interception refers to accessing and examining the content of, live or stored, communications. Content is defined as the part of a communication that conveys meaning (s. 261(6); McKay, 2017, pp. 32–36). Interception is a well-established surveillance method and has not faced significant challenges. The IPA doubles the duration of relevant warrants from three to six months. It also allows for open-ended warrants that cover multiple people, organizations, or premises (Nomikos, 2017, pp. 115–116). Importantly, the regulation of interception provides the matrix for the regulation of all other techniques.

Unlike CD surveillance, interception, equipment interference, and bulk surveillance, are acknowledged by the government as intrusive. They are available on grounds (national security, countering serious crime, and economic security) that allow ample room for executive discretion.[9] They can only be accessed by a narrow set of state actors through an enhanced authorization process. For these surveillance methods, authorization involves three steps: first, a high ranking official in the investigatory authority applies for a warrant to a Secretary of State; then, a senior official acting on behalf of the Secretary authorizes the warrant, having considered its necessity and proportionality; finally, a Judicial Commissioner applies judicial review principles on the Secretary's authorization. Warrants are valid for six months, but can be renewed through the same process for six-month periods infinitely. Finally, the IPA imposes on CSPs a duty to comply with warrants (s. 43), and penalizes disclosure of any feature of a warrant by CSP personnel or anyone who handles a warrant, including Intelligence personnel (ss. 57–58).

This general process varies across the three methods of surveillance with regard to exclusivity and the strictness of its thresholds. Interception is at the looser end of regulation, as nine agencies can apply for a warrant (s. 18).[10] Still, the application is directed from the top of these agencies (the Director) to the top of the relevant Department (Secretary or Minister) and must be approved by a Judicial Commissioner (s. 23 & 30). Finally, the IPA reinstates the blanket exclusion of intercepted material from being disclosed in open court, a standard Intelligence demand (s. 56; Schedule 3).

Equipment Interference

The Act legislates, for the first time, "equipment interference." The authorization protocol for it is the same with interception, except that the powers are available only to police and intelligence agencies (ss. 102–110).

Equipment interference is, essentially, hacking. It comprises two methods. The first, Computer Network Exploitation, enables Intelligence to access the total of a device's communications (CD and content), observe its internet browsing, uncover passwords, access stored files, read keystrokes, identify its location, etc. The second, Computer Network Attack, involves taking control of a device's functions: activate its microphones and cameras, undermine its encryption settings, modify communications' content, redirect internet browsing to sites the user had no intention to visit (and no knowledge that she has done so), and install files and programs. In this manner, Intelligence can not only find but also create evidence

(Anderson, 2015, p. 18, 137–138; Bowcott, 2015; GreenNet et al., 2015, p. 4, 8–9, 28; Privacy International, 2013).

Equipment interference is relatively new to the intelligence arsenal. Its existence came to light through the Snowden disclosures in 2013 and was tacitly acknowledged by the government in early 2015 (Anderson, 2015, p. 63, 332–333). Civil liberties organizations called for restricting and even outlawing it (Anderson, 2015, pp. 214–215, 227). Nonetheless, Intelligence (especially GCHQ and the Pentagon's NSA) treat it as an essential part of their operations and demanded its maintenance (Anderson, 2015, pp. 182–183, 199–200). In the IPA, these practices are officially acknowledged and legalized. Parliament brushed aside the acute privacy and entrapment concerns these methods raise to grant Intelligence its demands.

Bulk Surveillance

All techniques discussed thus far are directed toward defined targets. By contrast, bulk surveillance encompasses entire telecommunications systems absorbing all communications occurring through them without a specific target (Anderson, 2015, p. 128). It allows Intelligence to monitor millions of people it does not suspect of anything.

Bulk surveillance is not a separate method, but the employment of the other techniques *en masse*. Thus, the IPA provides for bulk interception (s. 136), bulk CD acquisition (s. 158), and bulk equipment interference (s. 176). The authorization protocol is virtually the same with that for interception (s. 138, s. 140, ss. 158–159, ss.178–179), except that bulk surveillance powers are restricted to intelligence agencies. Bulk interception and bulk equipment interference are only lawful when at least one end of the communication is situated outside the UK (s. 136 & 176). Yet, given that this requirement applies to blanket surveillance of entire systems, its value as a safeguard is unclear. Similarly, the requirement for proportionality seems to be inert as the mass nature of the surveillance makes a calculous of proportionality impossible (Anderson, 2016, pp. 28–29; Nomikos, 2017, p. 116).

Exposed in the Snowden files, bulk surveillance was under pressure in civil society and in the courts. A first case (*Big Brother Watch et al*. v. *UK*) challenging bulk interception of communications by GCHQ on Article 8 grounds (right to privacy and family life) had been under consideration by the European Court of Human Rights since 2013. In September 2018, the Court found that, while bulk surveillance was not beyond a state's margin of appreciation, historic (pre-IPA) surveillance had been in violation of Art. 8, as it did not involve independent oversight.[11] The Court accepted that judicial oversight, which the IPA had meanwhile installed, is an "important safeguard against arbitrariness."[12] In 2015,[13] the ECJ indicated that bulk surveillance could be *per se* incompatible with the right to privacy (Anderson, 2016, p. 29). Even the Investigatory Powers Tribunal, a closed court dedicated to reviewing covert practices,[14] uniquely decided against Intelligence. In September 2017, it found that bulk surveillance predating March 2015[15] had been in violation of European Convention of Human Rights Art. 8.[16] Finally, in a decision issued less than a month after the IPA was enacted, the ECJ ruled that national legislation that allows for general and indiscriminate CD

retention or mass access to CD without prior judicial or administrative review, contradicts rights to privacy (Art. 7), private data protection (Art. 8), and freedom of expression (Art. 11) of the EU Charter of Fundamental Rights.[17]

Apart from privacy concerns, the courts base their opposition to bulk surveillance on the lack of adequate statutory basis for the practice. The Act provides precisely this legal basis and, by installing administrative and judicial controls, makes bulk surveillance compatible with rule of law requirements. In doing so, it vitiates the grounds for complaint and legally buttresses the indiscriminate monitoring of communications.

Beyond the courts, bulk surveillance raised strong opposition by US-based communication service providers concerned that UK surveillance practices would clash with constitutionally underpinned US privacy law (Anderson, 2015, pp. 60–65, 206–210; Quinn, 2015). CSPs installed universal encryption in their operational systems, curtailing Intelligence ability to conduct bulk surveillance, causing the GCHQ Chief to accuse them of becoming the "command and control network of terrorists" (Quinn, 2014) and to demand that their collaboration is placed on statutory basis (Anderson, 2015, p. 63, 194–195). The IPA obliged. It authorizes the Home Secretary to issue National Security Notices and Technical Capability Notices, commanding CSPs to carry out "any conduct" to facilitate "anything done" by an intelligence agency (s. 252). This includes the removal of any "electronic protection applied by … a relevant operator to any communications or data" (s. 253(5c)).

The legalization of bulk surveillance was *the* main demand by Intelligence in pre-IPA consultations (Anderson, 2015, pp. 199–200). Intelligence chiefs claim that their operational paradigm depends on bulk surveillance (Anderson, 2015, pp. 195–200, 2016, pp. 150–154). Accordingly, the IPA negotiates and resists judicial opposition, as well as that of powerful IT corporations, to fortify the operational model of Intelligence.

Total Intelligence

The operational model in question is known as "target discovery" (aka: "pattern revelation" and "connecting the dots") and has been predominant since the turn of this century. It comprises the scanning of vast amounts of communications to identify suspicion (Anderson, 2015, p. 103, 129–130, 195–196, 2016, p. 82, 94, 104, 112, 123, 152–155). Rather than targeting specific individuals suspected of espionage, terrorism, or high-level criminality, it seeks to perpetually monitor everyone, in all their interactions, to discover suspicious associations and behaviors. It therefore disengages investigation from suspicion and makes surveillance a perpetual activity encompassing society as a whole.

This shift of operational paradigm resulted from engagement with a new kind of enemy. In the cold war context where modern Intelligence was forged, the threat emanated from specific states, was promulgated through centrally controlled operatives, had clearly distinguishable domestic and foreign elements, comprehensible purposes, and standardized methods. By contrast, the threat that contemporary terrorism poses is diffused, can erupt anywhere, is carried