Christos Boukalas

Overcoming Liberal Democracy: 'Threat Governmentality' and the Empowerment of Intelligence in the UK Investigatory Powers Act

Abstract

The sudden rise of the socio-political importance of security that has marked the 21st century entails a commensurate empowerment of the intelligence apparatus. This article 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 legalises their operational paradigm. Further, the socio-legal dynamics that informed the Act lead the article to conclude that Intelligence has become a dominant apparatus within the state. The article 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 towards neutralising threats that are yet unformed. Regarding its effects on liberal democracy, the article 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.

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, 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: 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: 61; 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

[1] Liberty vs Home Office [2018] EWHC 975 (Admin), referring to IPA provisions concerning access to retained communications data (see below, p.6).

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 organisation.

Accordingly, this article moves beyond a conceptualisation 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 regards to the 'logic' of the state, i.e. the ontological and epistemological premises that inform governmental practice and help it cohere. To unwrap the implications of the IPA for liberal democracy, the article 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 article 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 article assesses the significance of Intelligence empowerment with regards 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: 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', i.e. 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

[2] Throughout the text, I spell 'Intelligence' with a capital *I* to refer to it as a *state apparatus*, comprising the totality of intelligence agencies. I spell 'intelligence' with a small *i* to refer to its operation and product.

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 neutralise it. This 'threat governmentality' is a departure from a liberal biopolitical logic towards 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 article 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: 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 (Snowden (undated); Lyon 2015: 15-42). 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 authorisation 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).

[3] Apart from Simon McKay's (2018) comprehensive technical analysis and a number of brief notes on particular details, there are, to my knowledge, only two substantive analyses of the Act, those by Tristan Goodman (2018) and Lukia Nomikos (2017). Despite their analytical merit, neither of these excellent articles provides a comprehensive outline of the IPA. Thus, outlining the Act here is not only necessary for the purposes of the ensuing analysis, but also for introducing the reader to the Act's content.

The Commissioners overview electronic surveillance practices (s.229) that cannot lawfully proceed without their approval. Indeed, most IPA clauses are dedicated to outlining the authorisation 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 programmes, applications and files used in the course of a communication (s.261(5)) (Anderson 2015: 96; McKay 2017: 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: 83). Surveillance is authorised 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 penalises 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, s.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 authorised 12-month retention and was scheduled to expire by the end of 2016 (Anderson 2015: 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: 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 regards 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 authorisation 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 authorisations (Anderson 2015: 176-179, 197; Privacy International 2015: 6).

The inclusion of weblogs expands the remit of CD surveillance, i.e. 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: 78-79, 221-222; 2016; International Commission of Jurists 2014; Goodman 2018: 7-8; McKay 2017: 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

[4] Digital Rights Ireland and Seitlinger and others, ECLI: EU:C:2014:238
[5] R(Davis and Watson) vs Home Secretary [2015] EWHC 2092 (Admin)
[6] Case C-698/15, para.107
[7] Involving over 500,000 applications per year (Smith 2016: 16-17)

they are not limited to combating serious crime and do not require independent authorisation for access to retained data[8]. Accordingly, the government is considering introducing a new administrative body to dispatch relevant authorisations, 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 Authorisation 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: 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, organisations or premises (Nomikos 2017: 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, 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 authorisation process. For these surveillance methods, authorisation 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 authorises the warrant, having considered its necessity and proportionality; finally, a Judicial Commissioner applies judicial review principles on the Secretary's authorisation. Warrants are valid for 6 months, but can be renewed through the same process for 6-month periods infinitely. Finally, the IPA imposes on CSPs a duty to comply with warrants (s.43), and penalises 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 9 agencies can

[8] Liberty vs Home Office [2018] EWHC 975 (Admin).

[9] These categories lack statutory definition. The government rejected the recommendation of parliament's Intelligence and Security Committee to define 'national security' by invoking the multifarious and changeable nature of *the threat* to national security- without reference to the nature of the thing to be protected (McKay 2017: 226). Interestingly, with regards to bulk surveillance, Intelligence sets its own grounds ('operational purposes') for relative warrants within the remit of the three broad categories. These 'operational purposes' are composed by Intelligence, approved and reviewed by the Secretary of State, and announced to the Intelligence and Security Committee (IPA, ss.142, 161, 183, 212; McKay 2017: 144-145, 156-157, 169-170, 191-192)

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, s.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 authorisation 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), install files and programmes. In this manner, Intelligence can not only find but also create evidence (Anderson 2015: 18, 137-138); Bowcott 2015; GreenNet et al 2015: 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: 63, 332-333). Civil liberties organisations called for restricting and even outlawing it (Anderson 2015: 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: 182-183, 199-200). In the IPA, these practices are officially acknowledged and legalised. Parliament brushed aside the acute privacy and entrapment concerns these methods raise in order to grant Intelligence its demands.

Bulk Surveillance

All techniques discussed thus far are directed towards defined targets. By contrast, bulk surveillance encompasses entire telecommunications systems absorbing all communications occurring through

[10] MI5, MI6, GCHQ, Defence Intelligence Service, National Crime Agency, Northern Ireland and Scottish Constabularies, MET, and HMRC

them without a specific target (Anderson 2015: 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 authorisation 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, s.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: 28-29; Nomikos 2017: 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. vs 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 (ECtHR) 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: 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

[11] Case of Big Brother Watch and Others vs the United Kingdom (Applications nos. 58170/13, 62322/14 and 24960/15), 13 September 2018.
[12] ibid, paras.318, 375-383
[13] C-362//21, Schrems v Data Commissioner ECLI:EU:C:2015:650, §94
[14] The Investigatory Powers Tribunal is a closed session court, comprising ten senior judges, to which citizens can refer complaints of interference with person, property, or communications by a public authority, and complaints of breech of human rights ensuing by covert techniques employed by a public authority (http://www.ipt-uk.com/section.aspx?pageid=1). It decides most cases without a hearing; it cannot disclose, not even to the claimant, that a hearing is scheduled; it cannot compel oral evidence; does not have to give reason for refusing cases or for finding against the claimant; cannot disclose the identity of the witnesses or the material they submit. It relies almost exclusively to information submitted by Intelligence, which it does not disclose to the claimants (Anderson, 2015: 239-240; Privacy International 2015: 9).
[15] In March 2015, the government amended the Computer Misuse Act to grant intelligence operators impunity for hacking.
[16] Privacy International vs Foreign Secretary et al. UKIPTrib IPT_15_110-CH. 8 September 2017; also: Privacy International 2015.

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: 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: 63, 194-195). The IPA obliged. It authorises the Home Secretary to issue National Security Notices and Technical Capability Notices, commanding CSPs to carry out "any conduct" in order 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 legalisation of bulk surveillance was *the* main demand by Intelligence in pre-IPA consultations (Anderson 2015: 199-200). Intelligence chiefs claim that their operational paradigm depends on bulk surveillance (Anderson: 2015: 195-200; 2016: 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 in order to identify suspicion (Anderson 2015: 103, 129-130, 195-196; 2016: 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, in order to discover suspicious associations and behaviours. It therefore disengages investigation from suspicion and makes surveillance a perpetual activity encompassing society as a whole.

[17] Tele2 Sverige ECLI:EU:C:2016:970

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 standardised methods. By contrast, the threat that contemporary terrorism poses is diffused, can erupt anywhere, is carried out by loose networks and lone actors, and employs an endless variety of methods towards indefinite ends. Thus, for the security apparatus, anyone can be - or become - a terrorist, any association can indicate a conspiracy and any action can be preparation for an attack. Accordingly, Intelligence needs to monitor everyone in all their activity[18]. Similarly, the ultimate purpose of Intelligence changes. It is no longer restricted to defending the integrity of the 'body politic'. Its function is "to contribute to public security, defined as a state of mind that gives confidence that the risks ahead are being managed to a point where everyday life – and investment in the future – can continue" (Omand 2010: 11). Thus, intelligence tends to become *total* (Boukalas 2014: 143-145): all-encompassing regarding both its targets and what it seeks to protect. The main limits to total intelligence were technological and legal. As cyber capabilities are rapidly developing to allow the harvesting and analysis of the totality of data society produces, the IPA lifts the legal obstacles to total intelligence.

Intelligence Empowerment and Political Pre-emption

In the IPA, the vindication of Intelligence positions against social and judicial opposition, as well as that of a powerful sector of capital, shows Intelligence determining the law that governs it. This points to an augmentation of its relative power within the state. The IPA is the latest manifestation of this empowerment that is also evident in the financing of Intelligence, in its relation to the police, and in criminal (especially counterterrorism) law.

Intelligence Empowerment

Between 2001 and 2008, the budget of UK intelligence almost doubled (Gill and Pythian 2012: 182). Subsequently, it has been rising by an average 6 percent yearly to reach £3billion in 2018, making Intelligence virtually the only state mechanism with a substantially growing budget in an era of severe public sector cuts[19]. These resources are mainly dedicated to personnel increase, especially analysts, and to developing technological capacity for information harvesting and analysis (Anderson 2015: 193; Mannigham-Buller 2007: 71; Omand 2010: 31-35; Wintour 2015). This high level of support is

[18] On the difference between the two types of threat, or rather - and this is what matters - the way the security apparatus perceives them: Motram 2007: 44; Omand 2010: 31-35.
[19] See: Security and Intelligence Agencies 'Financial Statement' to Parliament for financial years 2009-2010 to 2017-2018.

in contrast to significant reductions in police spending. It points to a recalibration of the security apparatus, as analytical intelligence capacity substitutes for a decline in traditional law enforcement functions.

This recalibration of the security apparatus is evident in the promotion of the analytically-informed and pro-active 'intelligence-led policing' as the predominant law-enforcement paradigm (Gill and Pythian 2012: 56; Ratcliffe 2008). The insertion of Intelligence logic to law enforcement is coupled in the UK with an institutional realignment: in the Counterterrorism Command, which comprises police officers working under the direction of MI5 personnel, Intelligence installs detachments in every regional police force in the country. While proliferating at ground level, intelligence operations are centralising at the top, indicating its augmented political importance. The Joint Intelligence Committee is elevated to Cabinet level and the Intelligence and Security Coordinator office brings the entire mechanism under the direct control of the Prime Minister (Hennessy 2007: 31, 39; HM Government 2010; Gill and Pythian 2012: 58, 65-67; Omand 2010: 98-100, 104-105, 109).

Moreover, counterterrorism enhances intelligence-informed sanctions. It strengthens the powers of the state with regards to proscription[20] and citizenship revocation[21], and concentrates these powers in the hands of the executive (Anderson 2013: 61; Cram 2009: 56-58; Lavi 2010; Rooney 2014). Similarly, powers to freeze, confiscate, and restrict the exchange of property are drastically strengthened by counterterrorism law[22] and concentrated in the executive (Anderson 2011: 7, 10-13, 28-30, 66; Donohue 2008: 145-146; Sproat 2010). These unilateral powers are exercised on information provided by intelligence. They thus subject the property, associations and citizenship of individuals to executive decisions based on secret, untested evidence.

Finally, UK counterterrorism resulted to a pre-emptive turn in criminal law. The latter seeks to arrest crime before it is committed, and relies on intelligence for its application (Ashworth and Zedner 2016: 179-190; Boukalas 2017; McCulloch and Pickering 2010: 13-17). The outstanding specimens of this type of law are the preparatory[23] and encouragement[24] offences and the Terrorism Prevention and Investigation Measures (TPIMs)[25]. Preparatory offences criminalise any conduct - including lawful conduct - that is found to be in preparation of an act of terrorism. Encouragement offences criminalise any form of expression as long as it is considered likely that someone in its audience would perceive it as an encouragement to commit, prepare or instigate terrorism acts. TPIM orders allow the Home Secretary to impose severe restrictions on the liberty, finances, associations,

[20] Terrorism Act 2000, s.3, ss.11-13; Terrorism Act 2006, s.21
[21] Immigration, Asylum and Nationality Act 2006, s.56; Immigration Act 2014, s.66
[22] Terrorist Asset-Freezing Act 2010
[23] Terrorism Act 2000, ss.57-58; Terrorism Act 2006, s.5
[24] Terrorism Act 2006, ss.1-2
[25] Terrorism Prevention and Investigation Act 2011; Counter-terrorism and Security Act 2015, ss.16-20.

communications, work, education, movement (etc) of individuals she suspects of engaging in terrorism-related activity, when she has not enough evidence to bring them to trial or wishes to keep this evidence secret. The implementation of these laws depends on intelligence. Intelligence determines whether hiring a car or taking photographs are preparations for a, however remote, terrorist act. It also gauges the predisposition of an audience and therefore the existence of an encouragement offence, and it determines who shall be placed under restrictive orders. The challenge to the legal system and the rule of law that this pre-emptive turn signifies is multifarious and well documented (Boukalas 2017; Donkin 2014: 8-9; McCulloch and Pickering 2009: 634; McCulloch and Pickering 2010: 21; Roach 2010: 51-53). It represents an institutional alignment of criminal law with Intelligence: the operational logic of the latter comes to inform the form and logic of the former.

The determination of legislation by Intelligence in the IPA, the partial colonisation of criminal law and policing by its logic, and the relative abundance of resources dedicated to it, signify that Intelligence has become a *dominant state apparatus.* It is a mechanism whose particular interests are supported and promoted by the state as a whole. Its logic is the predominant state logic, it helps state policy to cohere, and can be represented to coincide with the broader 'common good' (For the meaning, functional and institutional importance of the 'dominant state apparatus': Jessop 2012: 127; 2016: 67-69; Poulantzas 1978: 136-139).

Political Pre-emption

The empowerment of Intelligence ensues from the dramatic rise of security in the overall political agenda *and* the adoption of a security strategy that is predominately pre-emptive (Stampnitzky 2013: 165-185). Security strategy is premised on the dogma that "if we wait for threats to fully materialise, we will have waited too long" (Bush 2002). Instead, "even if there is just a one percent chance of the unimaginable coming due, act as if it is a certainty… It's not about our analysis, it's about our response" (Vice-president Cheney, cited in Suskind 2007: 62). Pre-emption is an action-oriented modality of power, aiming to neutralise threats before they materialise. The most dynamic components of the UK counterterrorism strategy seek to disrupt terrorist attacks before they occur, and to deny the necessary condition for the formation of the threat by stopping people from becoming 'radicalised' (HM Government 2018).

Pre-emption is a management of future potentialities. It aims to enhance some and repress or erase others. It is an intervention aimed at neutralising a threat by altering the conditions that generate it. Pre-emption is therefore a preventive intervention. Yet, whereas prevention intervenes in partly identified causes of defined threats, pre-emption is founded on the premise of the unknowability of threats and their causes. Whereas prevention is a knowledge-based management of risk, pre-emption manages threats on the basis of uncertainty (de Goede and de Graaf 2013: 316). Unlike prevention,

pre-emption does not have a specified object of reference or objective. It is a logic that operates in and for itself. It is founded on the endemic character of hypothetical, unknown threats. It assumes the threat as an ontological condition co-expansive with society's potentiality (Massumi 2015: 27).

A maxim of former US Defence Secretary Donald Rumsfeld encapsulates pre-emptive logic, its agnosticism regarding the form of the threat and the certainty regarding its presence:

> "Reports that say that something hasn't happened are always interesting to me, because as we know, there are known knowns; there are things we know we know. We also know there are known unknowns; that is to say we know there are some things we do not know. But there are also unknown unknowns - the ones we don't know we don't know".

Accordingly, "the absence of evidence is not evidence of absence" (Rumsfeld 2002). The threat maybe intangible, imperceivable, and unknowable but its existence is certain. Total intelligence operationalises pre-emptive logic. If the threat is an ontological given, unknown, unknowable and impossible to disprove, it follows that the quest for knowledge must encompass the absence of evidence, survey the totality, and universalise suspicion.

Finally, the target of pre-emption, the thing it seeks to condition and selectively neutralise, is politics. Terrorism is legally defined as an unlawful act that is politically motivated, or aims to a political result [26]. Correspondingly, Intelligence is constituted as a mechanism that secures representative democracy from political subversion and industrial action (Donohue 2008: 194). Currently, in its iteration as *total*, it makes its mission to preserve "social normality" (Omand 2010: 320, 324). Thus, political conviction is the criterion for identifying suspicion when Intelligence employs its surveillance powers (McCulloch and Pickering 2009: 634) and it determines whether an offence actually exists when dealing with encouragement or preparatory offences (Tadros 2007: 684). In short, counterterrorism associates antagonistic politics with terrorism and Intelligence seeks to pre-emptively neutralise its potentiality. This is strikingly evident in the UK counter-extremism strategy. The government defines extremism as anything that deviates from political liberalism, and intervenes at the most intimate level of the individual's idea-formation in order to prevent the formation of non-liberal political subjectivities (Boukalas 2019).

Taking the IPA as our entry point, we have seen that Intelligence has become a dominant state mechanism; that this is due to a strategic turn to pre-emption that encompasses the state and law; and that its overall mission is to pre-emptively neutralise antagonistic politics. These developments implicate key features of liberal democracy, including the rule of law. Their implications are discussed in the following sections.

[26] Terrorism Act 2000, s.1

Intelligence vs the Rule of Law

During its drafting, Members of Parliament referred to the IPA as 'the snooper's charter', considered it a draconian affront to civil and privacy rights, and seemed reluctant to vote for it (Boffey 2015; Travis 2012; 2016). The government managed to secure a majority by installing judicial control over the powers it granted to Intelligence. However, this may not be a substantial safeguard. To begin with, the IPA outlines an authorisation regime full of loopholes: the grounds for a request are vague and over-broad and authorisations regarding CD are self-issued. Confusingly, the authorisation standards are in fact those of judicial review: judicial commissioners can only refuse approval on grounds of irrationality and illegality, and assessing proportionality with regards to bulk surveillance is absurd (Nomikos 2017: 118; Woods 2017: 103-105).

Moreover, the courts' track record on intelligence matters provides cause for scepticism regarding the robustness of judicial control. In its 15 years of pre-IPA existence, the IPT displayed an almost unspoiled record of decisions vindicating Intelligence. It only admitted a small fraction of complaints and, out of the 1,673 complaints it did admit, it upheld only ten (Anderson 2015: 121-123; Privacy International 2015: 9). In February 2016, in a case alleging the mass infliction of servers with malware, the IPT ruled that bulk equipment interference was lawful as long as it had statutory basis, regardless of whether judicial review was involved[27]. In the US, the Foreign Intelligence Surveillance Court, established in 1978, approves virtually all Intelligence requests, including authorisations for bulk surveillance on broad grounds (Boukalas 2014: 70; Elington 2016: 48; Greenberg 2016: 22-23) - something that bodes ill for the prospects of UK judicial commissioners to curtail Intelligence.

There are structural reasons underlying the courts' behaviour. Stemming from a traditionalist understanding of the division of powers, there is ingrained judicial deference to the executive in matters of national security (Donohue 2008: 326-330; Hadjimatheou 2017: 284; McKay 2017: 226-227). Moreover, given the adversarial nature of the British justice system, judges lack investigatory training and experience, and the necessary (legal, administrative and material) infrastructure that would enable them to meaningfully control Intelligence is also absent (Anderson 2015: 238). Crucially, the factual basis for an IPA s request derives exclusively from Intelligence. The judge has no grounds to second-guess it and may even be unaware of it. Instead, in considering approval, the judge is bound by the State Secretary's *assessment* of it, which she subjects to judicial review principles. Yet, while judicial review involves an adversarial element, no such thing is allowed here - there are no representations from a party that would challenge the Secretary's assessment or the

[27] Privacy International vs. Foreign Secretary and GCHQ [2016] UKIPTrib 14_85-CH

facts informing it (McKay 2017: 207). Finally, as UK law traditionally offers erratic and weak protection for privacy (Anderson 2015: 73; Donohue 2008: 182-195), limits to Intelligence powers would be imposed by supra-national jurisprudence. European courts are more protective of privacy than their British counterparts (Anderson 2015: 19, 31-32, 75, 224) and pose significant challenges to Intelligence powers. In this light the IPA provision for a domestic appeal route to IPT decisions (s.243) can reduce admissibility grounds to supra-national courts. The persistence of government circles, spearheaded by the then Home Secretary and later Prime Minister Theresa May (BBC 2013; Mason 2015; May 2016), to dissociate the UK from European jurisprudence will remove legal limitations to intelligence powers.

Judicial involvement is therefore likely to legitimise - and therefore strengthen - Intelligence powers rather than curtail them. Yet, it was enough to dissipate Parliament's outrage regarding the IPA. This indicates that representatives are bearers of a thin understanding of the rule of law as a procedural issue. This understanding does not grasp the rule of law as a relationship both between the branches of the state *and* between the state and society[28]. Accordingly, it confuses the two distinct moves that the IPA effectuates. The IPA empowers the executive in relation to the other state branches *and* empowers the state-as-a-whole in relation to society. The introduction of judicial control (appears to) ameliorate the first, intra-state, imbalance but does not ameliorate the second.

While the rule-of-law coating helped Parliament swallow the pill of total intelligence, it does not lift the incompatibility between the logic of Intelligence and that of the rule of law. The purpose motivating Intelligence is the accumulation of knowledge on existing and potential threats. Intelligence is not concerned with lawfulness and unlawfulness nor does it seek to prosecute or determine guilt. Its constitutive code is the threatening/non-threatening (and, ultimately, the friend/enemy) binary, not the legal/illegal one. Accordingly, its operation is not guided or evaluated by legal principles, but by its effectiveness in neutralising threats (Ratcliffe 2008: 48, 56-57, 68-75, 164, 172, 177, 224). Crucially, whereas the legal/illegal determination of the legal system refers to individualised cases, the threatening/non-threatening determination of Intelligence applies to ever-expanding segments of society. The temporalities of Intelligence are also different from those of the justice system. The latter operates in procedural time, a uniform timeline punctuated into stages by pre-defined critical moments (charging, trial, verdict, sentencing). Intelligence operates on emergency time where prolonged accumulation of information alternates at random with sudden accelerated intervention. Moreover, whereas the justice system is past-oriented, bearing on cases of accomplished harm, Intelligence is future-oriented. It monitors communication and activity in order

[28] This is ultimately premised on a dogmatic liberal understanding of the separation of powers as antagonistic, resulting to their mutual curtailment. It ignores the potential of state-power expansion through the limitations on the respective powers of each branch. See: Barber 2001; Krygier 2018: 26-27; Möllers 2013: 40-50.

to identify potential threats and threatening potentialities (de Goede and de Graaf 2013: 319; Hadjimatheou 2017; Treverton 2011: 125-129). Finally, whereas the legal system requires publicity throughout its process (from legislation drafting to sentencing), the strategies, operations, interventions and products of Intelligence can exist only in secrecy. Public exposure would undermine operations, imperil personnel and render the acquired knowledge pointless (Omand 2010: 253-259).

Ultimately, this incompatibility between institutional logics bears on the contradictory principles founding the modern state. Intelligence logic pertains to *raison d'etat*, the preservation, by all means necessary, of the state's institutionality (Machiavelli, *The Prince* (2008a)); Schimtt 2014) and of the social order this institutionality organises and reproduces (Boukalas 2014: 13-18; Jessop 2016: 53-120; Poulantzas 1978: 44-45, 147-152). The rule of law - from its germinal iteration in Aristotle as the distinction between healthy and corrupt forms of government (*Politics* I (1992)); its tentative affiliation with democracy in Machiavelli (*Discourses* I (2008b)); its association with equality in the republican revolutions of the 18th century (Bloch 1996: 61-65; Paine, *Rights of Man* (2008)); to its employment in organising the private-public separation in liberalism (Locke, *Second Treatise* (2016)) - throughout its endless socio-historical configurations, this concept represents the point of view of the governed (Bloch 1996: 153-181) and entails a *limitation* to organised public force over them (Krygier 2018: 20-24; Loughlin 2010: 312-341).

The IPA represents a contradictory and uneven compromise between the rule of law and Intelligence. It legalises practices that defy rule of law requirements, disregard the individualisation of culpability, detach investigation from suspicion and lift limitations to state power over society. But it does so *in* law and requires judicial approval of the augmented powers. In short, it inserts the extra- and anti-legal logic of Intelligence into the rule of law framework. By doing so, it alters the meaning of the rule of law concept (Boukalas 2017). The IPA reflects a displacement of the superior principle that unifies and motivates the legal system, from the ideal of justice to the imperative of security. It indicates a reconfiguration of the concept of the rule of law, so that it no longer signifies limitations to state power but grants it licence.

Liberalism, Democracy and 'Threat Governmentality'

Starting with an outline of the Intelligence powers codified in the IPA, this article unwrapped the significance of the latter for juridico-political forms. It has shown that the overall achievement of the IPA was to entrench *total intelligence* - the omnivorous operational paradigm of the intelligence apparatus - when judicial decisions and social pressure had rendered it precarious. In vindicating Intelligence positions in the face of social and judicial challenge, the IPA is symptomatic of an empowerment of Intelligence, its elevation into a *dominant state mechanism*. This is due to the

increased importance of security amongst state policies and its strategic turn to *pre-emption*: a strategy premised on ontological certainty and methodological agnosticism, geared to neutralise threats before they are formed. Intelligence is the par excellence pre-emptive state apparatus. Its institutional logic is incompatible with that of the rule of law. The IPA, however, inscribes it *in* law, causing a realignment of the organisational core of law (from justice to security) and of the overall function of the rule of law framework (from limits to licence).

The reconfiguration of the rule of law points to shifts in the broader political form. The reminder of the article unfolds the implications of the empowerment of Intelligence for the liberal-democratic form. It proceeds in three steps. First, given that liberalism and democracy are different political projects that can be in synergy but also in conflict (Wagrandl 2018), the article distinguishes between the two, aiming to register the implications for each. Next, it focuses on relations of transparency and opaqueness to find that 'total intelligence' as codified in the IPA reverses both democratic and liberal arrangements of the public-private relation. Finally, the article addresses the question of state-logic, the ontological and epistemological premises that inform state power and help it acquire strategic direction. It claims that the empowerment of Intelligence signals the advent of a new 'threat governmentality', which accentuates the anti-democratic elements inherent in liberalism but to such an extent that liberalism is overcome.

Liberalism vs Democracy

Democracy is the political organisation based on the principle of freedom, understood as the self-institution and self-determination of society. It entails that all members of society have equal capacity to determine politics, i.e. the activities pertaining to the institution, organisation, direction, and administration of society (Brown 2015; Castoriadis 1997). In a democratic polity all political functions are absorbed by society. The egalitarian and self-determining impetus of democracy is, in turn, founded on autonomy, on the fundamental premise that society alone is responsible for its creation, institution, and history (Castoriadis 1991: 158-162).

Liberalism is the political project of the capitalist class (Kondyis 2015). That is to say, it articulates and organises the power of a class that does not seek to rule society through domination, but through leadership (Gramci 1971: 245-246). It is therefore a contradictory political ideology, comprising oligarchic and democratic elements in dynamic tension. Its core juridico-political relations and forms, including liberty and equality, are organised on the basis of individually owned property (Bobbio 1990: 79-84; Krayer 2017; Pashukanis 1989). Even so, they carry considerable democratic potential and make demands for substantive social equality difficult to resist (Poulantzas 1978: 90-92, 203-204; Thompson 1975: 258-259). To safeguard the property relation from democratic pressures, liberalism institutes the economy as a self-governed realm ruled by its own

laws and excludes political power from intervening in its development. Accordingly, the object of liberal politics is to manage society so that the autonomous development of the economy is secured (Foucault 2008: 16, 30-32, 61-62, 246-247, 282-283; Gardiner 2018). The separation of the economy from politics informs the defining premise of liberalism, i.e. the division of social life into a public and a private sphere (Debord 1994: 11-24) and the imposition of limits in the intervention of the former into the latter. In instituting politics as the management of society aiming to accommodate the development of the economy, liberalism institutes politics as a sphere of expertise. This is a paradoxical claim, implying the possibility of expertise on the universal: from the minutest details of individual life to their combination in great social aggregates and historic trends (Castoriadis 2002). Crucially, the assumption of political expertise implies that the ignorant masses should be excluded from political functions, which should be left to the experts. This quasi-platonic principle of government by experts constitutes the oligarchic core of liberalism. It is a mainstay in liberal thought across its (right/left, classic and neoliberal, statist and individualist) currents: from Hegel to Schumpeter, JS Mill to Hayek, Durkheim to Weber (Holligner 1996; Kahan 2003; Tomlinson 1990).

Taking liberalism and democracy as distinct registers, the article traces the implications of the empowerment of Intelligence for each, and for liberal democracy as a whole. It examines the political implications of shifts in the relation between 'public' and 'private' and in the logic of the state, to claim that the empowerment of Intelligence pertains to a new kind of governmental logic - one that eclipses democratic politics and intensifies the oligarchic elements within liberalism to the point that liberalism is transcended.

Reversing the Public - Private Relation

The rule of law is a decisive element of liberal democracy. It demarcates the moveable border between the public and the private. It sets out the ways in which they interact and arranges the framework of practice within each. In short, it institutes the two spheres as such, their distinction and their interrelation. More than demarcating and policing the border between the two spheres, the rule of law defines each. It institutes the private sphere as a set of relations between abstract-individual property holders and arranges the form of the state, its competencies, powers and limits thereof. In short, the liberal political project of an atomised private realm separated from the state and protected from it *and* for a state with defined and limited powers over society, is inscribed in, and shapes, the rule of law. However, the rule of law is not a thing, but an evolving social relation. It is created by social dynamics, and can be reshaped by them. It provides a broad outline of institutional arrangements, which allows for adjustments. While it predominately expresses a liberal political arrangement, it incorporates democratic perspectives. It can provide the springboard for democratic demands, and be

reshaped accordingly. It is, in short, a plastic framework that can accommodate and reflect changing social dynamics and state strategies (Neumann 1996).

The entrenchment of total intelligence into law in the IPA confirms the ability of the rule of law to accommodate state strategies and to be reshaped by them. But its reconfiguration is not headed towards a democratic, or a liberal, direction. Total intelligence effectively cancels privacy. It allows the state unrestricted access in the private sphere, an access that is geared towards coercion. Crucially, the reconfiguration of the rule of law, to license rather than limit state power, threatens the separation of the two spheres, indicating a state-form that diverges from liberalism. As for democracy, in effectively canceling the private sphere, total intelligence denies the necessary space for a democratic politics to develop outside the institutions of the state. In targeting political interaction and association, it combats precisely the development of politics unauthorised by the state.

Moreover, total intelligence constitutes a reversal of state-society relations of visibility and knowledge. Its legalisation in the IPA institutes the full transparency of society before the most opaque mechanism of the state. This cancels the elemental condition for democratic control, i.e. the transparency of state actions and plans (Bobbio 2006: 20; Scheuerman 2016: 307). It upends the democratic arrangement were state actors are placed "under almost direct surveillance" by the people (de Tocqueville in Bobbio 2006: 151). It also contravenes the liberal demand for relative opacity of society from the state (Scheuerman 2016: 307). Thus, total intelligence fully reverses the liberal-democratic condition. In the place of a private society and a public state, it installs an open, public society monitored by a private state.

From Biopolitics to Threat Governmentality

This reversal of the public-private relation between state and society is symptomatic of a shift in the 'logic' of the state, the ontological and epistemological premises that inform the modality of its power. The scope of social transparency encompasses everyone, in all our interactions, perpetually. It comprises minute-by-minute biographical accounts stretched out in longitude and intimately detailed singular accounts, combined into gross social averages. In short, the state knows every modicum of micro-life as it occurs, as well as the macro-social patterns and trends into which micro-events combine. Thus, total intelligence pertains to biopolitics, also known as 'the liberal way of rule' (Foucault 2008). It designates Intelligence as bio-power, set to know society in order to govern it through subtle interventions in its evolving patterns rather than top-down imposition of rules. However, total intelligence designates a departure from biopolitics.

The departure concerns the political epistemology informing state logic and the modality of state power. Liberal biopolitical power is premised on the knowability, measurability and, ultimately, calculability of social phenomena and their causes. It seeks to determine and influence them through

targeted, calculated, causal interventions. Total intelligence indicates an epistemological shift. It is designed to monitor threats that are unknown and stem from unknowable causes. Its epistemological foundation is not one of knowability, but one of radical uncertainty regarding the form and cause of the threat. It denies the possibility of determination and is not concerned with the causation of social phenomena. Indeed, un-knowability is the defining feature of the threat. If the threat were known it would not be a threat but a situation, something that can be managed. Its form is undefined and only exists as a futurity (Massumi 2015: 27, 30, 175; Stampnitzky 2013: 184-200; Zedner 2009: 45-46). The threat is therefore amorphous and spectral, perpetually shape-shifting, migrating and metastasising. It changes objectives, means and rationales. It is manifested unpredictably across space and inhabits every sphere of social activity. It is seldom actual or formed, but always in a process of emergence (Boukalas 2014: 51-56, 76, 90-95, 135, 155; Neocleous 2016: 2, 4, 38, 45, 69). Its spatial and temporal indeterminacy render it omnipresent. It is precisely the threat's spatio-temporal ubiquity that determines total intelligence and its 'discovery' approach. If any person and conduct can become a threat, it follows that the perpetual monitoring of all individuals in all their interactions is necessary to discover threatening potentialities. The amorphous nature of the threat, and the existential necessity to pre-empt it, define the methods of Intelligence: "GCHQ will not be able to identify those who wish us harm without bulk powers… Without them these threats will develop to fruition undetected until it was too late to stop them" (GCHQ 2016 in Anderson 2016: 152). Total intelligence is constant surveillance seeking to identify suspicion where, initially, there is none. Procedurally, this separates investigation from suspicion; politically, it means that, for the state, everyone is suspect. The only certainty about the unknowable threat is its existence. There *are* unknown unknowns (and 'the absence of evidence is not evidence of [their] absence'). If not pre-empted, the threat will materialise: the crisis will erupt, the enemy *will* attack (Neocleous 2015).

In short, the threat is an ontological condition of the social becoming. Accordingly, state power is not limited to calculated interventions between a phenomenon and its causes. It moves to arrest its potentiality before it is formed. It brings to bear on the ontogenic conditions of the threat, on the social formation that could generate it. It is not a bio-political management of species-being anymore but an onto-power that seeks to determine what 'species' will comprise the social (Massumi 2015: 40-41, 86). This onto-power is a departure from the 'liberal way of rule' towards a post- or neoliberal one. Indeed, neoliberal political theory sees the market not as a self-governed entity, but as one necessitating constant intervention for its formation and sustenance - one, in short, under perpetual threat to its existence and in permanent need of security (Harvey 2005: 64-86; Jessop 2016: 205-207; Mirowski 2009: 417-455; Tzouvala 2018: 123-126).

The epistemological shift that underpins the transition from bio- to onto-politics entails a change in the character of the (alleged) political expertise. Biopolitics is an instantiation of

government by experts (Boukalas 2013). It postulates a 'political science', an expertise on the universal, and assigns political functions to the experts, making society the object, not the subject, of government. Threat governmentality pertains to this heteronomous political imaginary but also reconfigures it, intensifying its antidemocratic character.

Threat governmentality displaces the core *object* of political expertise from the economy to security. This effectuates a closure of the politically relevant expertise. Economic expertise can be claimed by large segments of society and virtually everyone can claim some relevant knowledge through personal experience. It is therefore an open knowledge, contested and conflictual. By contrast, security, and the threat that informs it, is firmly beyond the knowledge of society and must remain so. Further, the transition to threat governmentality entails a shift in the *nature* of political expertise. Threat governmentality is a modality of power premised on the impossibility of certain knowledge and decipherable causalities and determinations, and its interventions are more creative than administrative. The *episteme* of threat anticipation is a "wholly unscientific project of crystal ball gazing" (McCullogh and Pickering 2009: 635). From expertise on the universal, we pass to expertise on the unknowable. Accordingly, this expertise is not based on technical-scientific rationality, but employs the latter to approach the truth and act on it intuitively: "it is not about our analysis - it's about our response" (Cheney in Suskind 2007: 62). Its intuitions and interventions are not systematically outlined, statistically informed, tested, and prospective. They are unverifiable, unfalsifiable, counterfactual, and contemporaneous. Moreover, the truth around which political expertise is organised - the threat - is 'too terrible' for common people to behold. Threat governmentality resembles the apocalyptic platonism of Leo Strauss, a secluded government by wise men, whose wisdom consists in knowledge of the evil rather than the good (Strauss 1968: 25-26; 1983: 178-188). Its archetype of the expert is not the scientist but the mystic. Threat governmentality is conservative in the pre- and anti-modern sense. It presumes society as incapable of governing itself, incapable of even knowing the premises and practices of its government. The latter is resumed by secretive experts with esoteric knowledge of a threat that is unknowable in its essence.

Thus, threat governmentality fulfils the anti-democratic potential of expertise-based politics. By substituting rationality for mysticism at the core of governmental logic it bases the relation between society and its government on blind faith. Society is meant to have unconditional trust on the intentions and practices of a state that considers it suspect. Threat governmentality negates the fundamental premise of democratic politics: that society institutes and governs itself. With regards to liberalism, its implications are paradoxical. It intensifies the core oligarchic aspect of liberalism, the exclusion of society from politics and its resumption by political experts. But, in setting political expertise on an anti-rational basis and setting it to stifle political antagonism, it outlines a conservative political constellation that defies liberalism. Yet, this conservative governmentality is developed in

order to secure liberal politics by pre-empting the possibility of political change. Threat governmentality poses a paradox: the liberal political *institution* is perpetuated by outcasting the liberal political *logic*. Liberalism is transcendent in order to be secured.

Conclusion: Towards a Critique of Threat Governmentality

The prominence of security policy that marks the 21st century and the predominance of a pre-emptive approach therein, considerably strengthen the position of Intelligence within the state. The IPA emphatically confirms this empowerment. It legalises surveillance powers that are extraordinary in scope and intensity and does so in the face of social resistance and judicial challenge. The overall achievement of the IPA is the legalisation of the prevailing operational paradigm of Intelligence that consists of perpetual monitoring of social interaction in order to discover potential threats. The empowerment of Intelligence results from the adoption of pre-emption as the defining security strategy, a strategy that is premised on the unknowability of threats and intervenes to prevent their formation. This is the first set of claims advanced in this article.

A second set of claims refers to the political implications of the empowerment of the state's most unaccountable mechanism. Drawing from legal and political theory the article notes the incompatibility of the logic of Intelligence with the rule of law and the colonisation of the latter by the former. This, in turn, is seen as an element in a broader reconfiguration of political logic towards a governmentality based on threat. It involves the hollowing out of the rule of law framework and a reversal of its political meaning. It also involves a reversal of relations of transparency between the state and society and a shift from bio-power to onto-power. From measured, calculated, and projective interventions aiming to enhance economic performance, governmental logic moves to unrestrained pre-emptive interventions premised on the impossibility of knowledge and determination of social phenomena that are conceptualised as ontologically threatening. The first two reversals (regarding the rule of law, and relations of transparency) upset both democratic and liberal political principles. The shift to threat governmentality denies the most elemental condition of democratic politics. It also intensifies the core oligarchic principle of political liberalism to the point that liberalism is transcended - it employs a conservative, anti-liberal political imaginary to safeguard the liberal political institution.

Thus, the empowerment of Intelligence that the IPA codifies and the threat governmentality to which this empowerment pertains, point to a mutation of liberal democracy into a political order that is anti-democratic and difficult to classify as liberal. This represents a shift much more profound than an infringement of privacy rights. It represents a transfiguration of the political order to which these rights pertain. Attempts to defend privacy rights *per se* address the state in a language it no longer

cares to understand. Instead, the defence of privacy rights can only occur by reclaiming democratic (or, at least, liberal) politics. This must involve a demystification of threat governmentality, its assumptions and objectives, starting with its organisational category, the threat.

The threat is the ghost that animates the new governmentality. The state sees individuals as suspects of uncommitted crimes and society as dangerous: the threat lies in the potentiality of the social. But, rather than being a spectral, mystical entity, the threat, like everything else, is produced in and by society. Hence the perpetual monitoring of social interaction by Intelligence that the IPA accommodates. Crucially, the occult threat is identified. For the UK the threatening subjectivity is the 'extremist', defined as the anti-liberal, the person who contravenes the key premises of political liberalism (Boukalas 2019). In the US, the bearer of all threat is the Universal Adversary, i.e. the total of 'foreign terrorists', 'state-sponsored adversaries', 'domestic radical groups', and 'disgruntled employees' (Boukalas 2014: 205; 2015: 55-71; Neocleous 2015; 2016). The threat is the enactment of antagonistic politics. What must be pre-emptively neutralised is the political potential of society, its capacity to envision and strive for change. The objective of threat governmentality is to impose political stasis.

Threat governmentality, and the post-liberal and anti-democratic mutation it entails, is a sign of a weakening state. The institution of the threat at the heart of governmental logic points to a state that fears society. Perceived as threatening, the indeterminacy of social dynamics generates the need for the fullest possible knowledge of society - hence the rise of Intelligence and the inscription of its total powers in law. The threat is always *in potentia*. This means that the state conceptualises the future as a threat. By the thorough knowledge of society and the political focus of this knowledge, it seeks to pre-empt the potential for a political future. This points to a foreclosure of the future by a fearful state. It points to the moment when liberal democracy is corrupted into an authoritarian republic[29].

[29] On neoliberalism as a negation of political liberalism: Chandler 2016: 13. On authoritarianism as a corrupted form of liberalism: Hayek 1960: 103.

Acknowledgments

The author is grateful to Phil Thomas (Cardiff and Northumbria) and Anna Tilling (Tübingen) along with everyone that participated in the *Internationales Zentrum für Ethik in den Wissenschaften* workshop on 'Surveillance, Terrorism, Normality?' for invaluable feedback on previous iterations of this article. He also wishes to thank Annette Morris (Cardiff) and David Sugarman (Lancaster) for their critical and encouraging comments.

References

Amnesty International (2016) 'Written Evidence for the Joint Committee on the Draft Investigatory Powers Bill' IPB0074. *House of Parliament Joint Committee on the Investigatory Powers Bill* (https://www.parliament.uk/documents/joint-committees/draft-investigatory-powers-bill/written-evidence-draft-investigatory-powers-committee.pdf)

Anderson, D (2011) 'Report on the Operation in 2010 of the Terrorism Act 2000 and of Part 1 of the Terrorism Act 2006'. *Independent Reviewer of Terrorism Legislation*. London: HM's Stationary Office.

Anderson, D (2013) The Terrorism Acts in 2012. *Independent Reviewer of Terrorism Legislation*. London: HM's Stationary Office, July.

Anderson, D (2015) 'A Question of Trust – Report of the Investigatory Powers Review'. *Independent Reviewer of Terrorism Legislation*. London: HM's Stationary Office.

Anderson, D (2016) 'Report of the Bulk Powers Review'. *Independent Reviewer of Terrorism Legislation*. London: HM's Stationary Office

Aristotle (1992) *Politics* [c.335 BC]. London: Penguin

Ashworth, A and Zedner, L (2015) *Preventive Justice*. Oxford: OUP

Barber, N.W (2001) 'Prelude to the Separation of Powers' *Cambridge Law Journal* 60(1): 59-88

BBC (2013) 'Theresa May: Tories to Consider Leaving European Convection of Human Rights', 9 March

Bloch, E (1996) *Natural Law and Human Dignity*. Cambridge, Ma.: MIT Press

Bobbio, N (1990) *Liberalism and Democracy*. London: Verso

Bobbio, N (2006) *Democracy and Dictatorship*. Cambridge: Polity

Boffey, Daniel (2015) 'Theresa May Keeps Snooper's Charter Secret'. *The Guardian*, 13 June

Boukalas, C (2013) Government by Experts: Counterterrorism Intelligence and Democratic Retreat. *Critical Studies on Terrorism* 5(2): 277-296

Boukalas, C (2014) *Homeland Security, its Law, and its State*. Abington: Routledge

Boukalas, C (2015) ‘Class War on Terrorism: Counterterrorism, Accumulation, Crisis’. *Critical Studies on Terrorism* 8(1): 55-71.

Boukalas, C (2017a) ‘UK Counterterrorism Law, Pre-emption and Politics: towards “Authoritarian Legality”?’. *New Criminal Law Review* 20(3)

Boukalas, C (2019) ‘The Prevent Paradox: Destroying Liberalism in Order to Protect it’ (2019) *Crime, Law and Social Change*. https://doi.org/10.1007/s10611-019-09827-8

Bowcott, O (2015) ‘GCHQ Accused of “persistent” Illegal Hacking at Security Tribunal’. *The Guardian*, 1 December

Brown, W (2015) *Undoing the Demos*. New York: Zone

Bush, GW (2002) ‘President Bush Delivers Graduation Speech at West Point’. *The White House Archives*, 1 June

Castoriadis, C (1997) ‘The Greek Polis and the Creation of Democracy’. In D.A Curtis (ed) *The Castoriadis Reader*. Oxford: Blackwell

Castoriadis, C (1991) ‘Power, Politics, Autonomy’. *Philosophy, Politics, Autonomy*. Oxford: OUP

Castoriadis, C (2002) *On Plato’s Statesman*. Stanford: SUP

Chandler, D (2016) ‘Debating Neoliberalism: Exhaustion of the Liberal Problematic’ in D. Chandler and J. Reid *The Neoliberal Subject*. London: Rowman & Littlefield

Cram, I (2009) *Terror and the War on Dissent*. London: Springer

Debord, G (1994) *The Society of the Spectacle*. New York: Zone.

de Goede, M and de Graaf, N (2013) ‘Sentencing Risk: Temporality and Precaution in Terrorism Trials’ *International Political Sociology* (2013) 7, 313-331

Donkin, S (2014) *Preventing Terrorism and Controlling Risk – a Comparative Analysis of Control Orders in the UK and Australia*. London: Springer

Donohue, L (2008) *The Cost of Counterterrorism.* Cambridge: CUP

Ellington, Thomas (2016) ‘Secrecy Law and its Problems in the United States’. In G. Martin et al *Secrecy, Law and Society*. Abington: Routledge

Foucault, M (2008) *The Birth of Biopolitics*. Basington: MacMillan

Gardiner, M (2018). ‘Thatcherism as an Extension of Consensus’ in B. Golder and D. McLaughlin (eds) *The Politics of Legality in a Neoliberal Age*. Abington: Routledge

GCHQ (2016) ‘Statement of Utility of Bulk Capabilities’ in Anderson (2016) ‘Report of the Bulk Powers Review’. *Independent Reviewer of Terrorism Legislation*. London: HM’s Stationary Office.

Gill, P and Phythian, M (2012) *Intelligence in an Insecure World*. Cambridge: Polity

Goodman, T (2018) ‘The Investigatory Powers Act 2106: a Victory for Democracy and the Rule of Law?’ *Bristol Law Review* 5 (1), 2-26

Gramsci, A (1971) *Selections from the Prison Notebooks*. London: Lawrence and Wishart

Greenberg, Karen (2016) *Rogue Justice*. New York: Crown

GreenNet et.al. 'Amended Statement of Grounds' (2015) Investigatory Powers Tribunal (https://regmedia.co.uk/2015/12/01/greenet_amended_grounds_filed.pdf) 19 May

Hadjimatheou, K (2017) 'Neither Confirm nor Deny: Secrecy and Disclosure in Undercover Policing' *Criminal Justice Ethics* 36 (3), 279-296

Harvey, D (2005) *Neoliberalism*. Oxford: OUP

Hayek, FA (1960) *The Constitution of Liberty*. Chicago: UCP

Hennessy, P (2007) 'From Secret State to Protective State'. In P. Hennessy (ed) *The New Protective State*. London: Continuum

HM Government (2010) *National Intelligence Machinery*. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61808/nim-november2010.pdf; accessed 3 April 2017

HM Government (2018) *CONTEST. The United Kingdom's Strategy for Countering Extremism*. Cm 9608. London: HM Stationary Office

Hollinger, R (1996) *The Dark Side of Liberalism*. Westport, CT: Praeger

International Commission of Jurists (2014) 'Written Submissions re: *Big Brother Watch et al v the United Kingdom*'. 9 February

Jessop, B (2012) *State Power. A Strategic-Relational Approach*. Cambridge: Polity

Jessop, B (2016) *The State – Past, Present and Future*. Cambridge: Polity

Kahan, A (2003) *Liberalism in Western Europe*. Basingstoke: Palgrave Macmillan

Kondylis, P (2015) *Conservatism*. Herakleio: Crete University Press (in Greek; original title: *Konservatism*. Klett-Cotta 1986)

Kraver, Tor (2017) 'Law, Development and Political Closure under Neoliberalism'. In H. Brabazon (ed.) *Neoliberal Legality*. Abington: Routledge

Krygier, M (2018) 'Transformations of the Rule of Law' in B. Golder and D. Mcloughlin (eds) *The Politics of Legality in a Neoliberal Age*. Abington: Routledge

Lavi, S (2010) Punishment and the revocation of citizenship in the United Kingdom, United States and Israel. *New Criminal Law Review* 13 (2): 404-426

Liberty (2015) 'Liberty - Written Evidence on the Investigatory Powers Bill' IPB14. *House of Parliament Joint Committee on the Investigatory Powers Bill* (https://www.parliament.uk/documents/joint-committees/draft-investigatory-powers-bill/written-evidence-draft-investigatory-powers-committee.pdf)

Locke, J (2016) *Second Treatise of Government* [1683]. Oxford: OUP

Loughlin, M (2010) *Foundations of Public Law*. Oxford: OUP

Lyon, D (2015) *Surveillance after Snowden*. Cambridge: Polity

Machiavelli, N (2008a) *The Prince* [1532]. Oxford: OUP

Machiavelli, N (2008b) *Discourses on Livy* [1531]. Oxford: OUP

Manningham-Buller, E (2007) 'The Terrorist Threat to the United Kingdom'. In P. Hennessy (ed) *The New Protective State*. London: Continuum

Mason, R (2015) 'Human Rights: Tories Reject Reports of Rift between Cameron, May and Gove'. *The Guardian*, 1 June

Massumi, B (2015) *Ontopower*. Durham: Duke UP

May, T (2016) 'Theresa May's Speech on Brexit' *Conservative Home*, 25 April (https://www.conservativehome.com/parliament/2016/04/theresa-mays-speech-on-brexit-full-text.html)

McCulloch J and Pickering S (2009) Pre-crime and Counterterrorism – Imagining Future Crime in the War of Terror. *British Journal of Criminology* 49(5): 628-645.

McCulloch, J and Pickering S (2010) 'Counter-terrorism: the Law and Policing of Pre-emption'. In McGarrity N, Lynch A and Williams G (eds) *Counterterrorism and Beyond - the Culture of Law and Justice after 9/11*. Abington: Routledge, pp.13-29

McKay, S (2017) *Blackstone's Guide to the Investigatory Powers Act 2016*. Oxford: OUP

Mirowski, Philip (2009) 'Postface'. In P. Mirowski and Dieter Plehwe (eds.) *The Road from Mont Pelerin*. Harvard UP, 417-455

Möllers, C (2013) *The Three Branches*. Oxford: OUP

Mottram, R (2007) 'Protecting the Citizen in the Twenty-first Century: Issues and Challenges'. In P. Hennessy (ed) *The New Protective State*. London: Continuum

Neocleous, M (2000) *The Fabrication of Social Order: A Critical Theory of Police Power*. London: Pluto

Neocleous, M (2008) *Critique of Security*. Edinburgh: EUP

Neocleous, M (2015) 'The Universal Adversary Will Attack: Pigs, Pirates, Zombies, and the Class War. Critical Studies on Terrorism 8(1): 15-32

Neocleous, M (2016) *The Universal Adversary*. Abington: Routledge

Neumann, F (1996) The change in the function of law in modern society. In W. E. Scheuerman (Ed.), *The Rule of Law under Siege*. Berkeley: University of California Press.

Nomikos, L (2017) 'Are we Sleepwalking into a Surveillance Society? *Bristol Law Review* 4, 111-128

Omand, D (2010). *Securing the State*. London: Hurst

Paine, T (2008). Rights of Man [1791-1792]. Oxford: OUP

Pashukanis, E (1989) *Law and Marxism - A General Theory*. London: Pluto

Poulantzas, N (1978) *State, Power, Socialism*. London: Verso

Privacy International 'Statement of Grounds (2013) Investigatory Powers Tribunal (https://privacyinternational.org/sites/default/files/2018-03/2013.07.08%20Privacy%20International%20IPT%20Grounds.pdf) 8 July

Privacy International (2015) 'The Right to Privacy in the United Kingdom'. London: PI

Quinn, B (2015) 'UK Surveillance Bill Could Bring "very dire consequences" Warns Apple Chief'. *The Guardian*, 10 November

Quinn, B et al (2014) 'GCHQ Chief Accuses US Tech Giants of becoming Terrorists; "networks of choice"'. The Guardian, 3 November

Ratcliffe, J (2008) *Intelligence-led Policing*. Cullompton: Willian

Roach, K (2010) 'The Eroding Distinction between Intelligence and Evidence in Terrorism Investigations'. In McGarrity N, Lynch A and Williams G (eds) *Counterterrorism and Beyond - the Culture of Law and Justice after 9/11*. Abington: Routledge, pp.46-68.

Rooney, C (2014) Stateless terrorist: citizenship in an age of risk. *Border Criminologies* (http://bordercriminologies.law.ox.ac.uk/citizenship-in-an-age-of-risk/; accessed 10 April 2016)

Rumsfeld, D (2002) *US Department of Defence News Briefing*, 12 February

Scheuerman, W.E (2016) 'Digital Disobedience and the Law'. *New Political Science* 38(3): 299-314

Schmitt, C (2016) *Dictatorship*. Cambridge: Polity

Smith. G (2016) 'The Proposed Changes to the UK Investigatory Powers Act' *Privacy and Data Protection* 18, 16-17

Snowden, E (undated) Snowden Digital Surveillance Archive (https://snowdenarchive.cjfe.org)

Sproat, P (2010) 'Counter-terrorist finance in the UK: a Quantitative and Qualitative Commentary Based on Open Source Materials'. *Journal of Money Laundering Control* 13(4): 315-335

Stampnitzky, L (2013) *Disciplining Terror*. Cambridge: CUP

Suskind, R (2007) *The One Precent Doctrine*. London: Pocket Books

Strauss, L (1968) *On Tyranny*. New York: Cornell University Press

Strauss, L (1983) *Studies in Platonic Philosophy*. Chicago: UCP

Tadros, V (2007) 'Justice and Terrorism'. *New Criminal Law Review* 10(4): 658-689

Thompson, EP (1975) *Whigs and Hunters*. New York: Pantheon

Tomlinson, J (1990) *Hayek and the Market*. London: Pluto

Travis, A (2012) 'Snooper's Charter Proposal Sparks Tory Row'. *The Guardian*, 14 June

Travis, A (2015) 'Security Services' Powers to be Extended in Wide-ranging Surveillance Bill'. *The Guardian*, 27 May

Travis, A (2016) ‘Home Office to Publish Revised Draft of Snooper’s Charter’. *The Guardian*, 1 March

Treverton GF (2011) *Intelligence for an Age of Terror*. Cambridge: CUP

Tzouvala, N (2018) ‘Neoliberalism as Legalism’ in B. Golder and D. Mcloughlin (eds) *The Politics of Legality in a Neoliberal Age*. Abington: Routledge

Wagrandl, U (2018) ‘Transnational Militant Democracy’ *Global Constitutionalism* 7(2): 143-172

Weaver, M (2016) ‘MI5 Resists Independent Oversight of Bulk Data Collection’. *The Guardian*, 26 July

Wintour, P (2015) ‘David Cameron to Boost Security Spending after Paris Attacks’. *The Guardian*, 15 November

Woods, L (2017) ‘The Investigatory Powers Act 2016’. *European Data Protection Law Review* 3, 103-105.

Zedner, L (2009) ‘Fixing the Future? The Pre-emptive Turn in Criminal Justice’. In B. McSherry, A. Norrie, and S. Bronitt (eds.) *Regulating Deviance* Oxford: Hart