Privatized Counter-Terrorist Surveillance: Constitutionalism Undermined

Fiona de Londras

1 INTRODUCTION

This chapter is concerned with the constitutionalist challenges posed by privatized counter-terrorist surveillance (PCTS). PCTS is defined here as surveillance done for the purposes or in the course of a broader counter-terrorist regime and in which private (by which is meant non-state) actors are involved. This chapter characterizes PCTS as one illustration of a broader trend of privatization in counter-terrorism and problematizes it as a phenomenon that severely undermines the core constitutionalist commitment to limited, transparent and accountable power.

The concentration here is not on the particular rights infringements or liberty interferences that PCTS might give rise to (such as privacy violations); nor is it on cataloguing the multiple ways in which law has appeared to be incapable of 'managing' this phenomenon.[1] Rather, this chapter takes a 'bigger picture' approach and aims to expose both the phenomenon of PCTS and its counter-constitutionalism for the purposes of arguing that what is required to respond appropriately to this (and indeed other counter-terrorist trends of concern) is not 'more law' per se. What is required is a fundamental recommitment to constitutionalism that, more than a decade into an intense period of transnational securitization, still appears to be lacking.

---

[1] On both see, eg, S Chesterman, *One Nation under Surveillance: A New Social Contract to Defend Freedom Without Sacrificing Liberty* (New York: Oxford University Press, 2011).

This chapter first outlines the general phenomenon of privatized counter-terrorism, which I characterize as both widespread and problematic. In the first section I identify four kinds of privatized counter-terrorism observable in the current context: open privatization, closed privatization, statutory privatization and non-contractual co-option. While all of these are problematic in different ways, I concentrate particularly on closed privatization and non-contractual cooption which are both widespread in the surveillance context and of particular constitutionalist concern. Having outlined the patterns of PCTS in the third section, I go on to identify what I consider to be the core counter-constitutionalist dilemmas posed by PCRS: the relatively unlimited nature of what is considered 'legitimate' private power when compared with clear constitutionalist power limitations imposed on states, the lack of transparency and its attendant imperative for justification, and the accountability gaps that this gives rise to. These are, I argue, severe constitutionalist concerns, perhaps most particularly because they point to the limited capacity of *law* to effectively address them.

2 PRIVATISED COUNTER-TERRORISM: THE CONCEPT AND CATEGORIES

Privatization is a complex concept and has been the subject of sustained debate and academic attention across disciplines.[2] Leaving the complex contestations as to the meaning of 'private' to one side, however, we can usefully concentrate here on what Lundqvist describes as the minimum definition of privatization, that is, moving or transferring something that has hitherto been within the public sector into the private

[2] For a sample of the rich literature see, eg, D Parker and D Saal (eds), *International Handbook on Privatization* (Cheltenham: Edward Elgar, 2003).

sector.[3] This definition, and indeed the discussion throughout this entire chapter, relies on a relatively simplistic distinction between public (or governmental/state) actors and private (or non-state) actors which can itself be problematized. However, that is a task undertaken elsewhere.[4] For the purposes of this chapter it is sufficient to proceed with this crude distinction, theoretically unsatisfactory as it may be, largely because that is how law *generally* distinguishes between the two.

Over recent decades, it has become increasingly common for states to privatize functions that were traditionally undertaken by public actors. These functions range from the provision of health care to the regulation and provision of energy, water and telecommunications to matters as central to the state as the deprivation of liberty by means of imprisonment. Counter-terrorism has not escaped this trend. Across a wide range of counter-terrorist activity we can see the involvement of private (largely but not exclusively) corporate actors such as private security companies, aviation and other logistics enterprises, and central banks. When we remind ourselves that states are essentially involved in both *providing* for their people and *producing* services, and that security is one such (if not the core) service the state provides and produces, this privatization of counter-terrorism was perhaps inevitable.

Kolderie has identified three dimensions across which privatization generally occurs: (1) government decides to provide something but involves a non-state actor in

---

[3] L J Lundqvist, 'Privatization: towards a concept for comparative policy analysis' (1988) 8 *Journal of Public Policy* 1, 6.

[4] F de Londras, *Privatised Sovereign Performance, Counter-Terrorism and Endangered Rights* (Cambridge: Cambridge University Press, forthcoming 2014) ch 1.

production of the services required for such provision; (2) a non-state actor decides to provide something and enlists government in producing the required services; or (3) both the decision to provide and the production of the required services are taken by a non-state actor.[5] He goes on to illustrate these three dimensions in the context of security by pointing to instances where government decides to provide security at an event and then contracts with a private corporation to actually produce the security (evoking (1) above), or a private actor decides that security is required for an event and then engages with the government for it to be produced by state actors (evoking (2) above), or a private actor decides that it wants to provide security and contracts with a private corporation for that security to be produced (evoking (3) above).[6]

We also observe these three dimensions in the more acute security scenario of counter-terrorism. Take, for example, the enlisting of central banks and transaction tracking companies in the implementation of legal frameworks for the disruption of terrorist financing (referring to scenario (1) above),[7] or the enlisting of the military (including the placement of weaponry on residential buildings) to provide security for the London Olympics (scenario (2) above),[8] or the engagement by private companies of private security firms and technology to protect against cyber-terrorism (scenario

---

5 T Kolderie, 'The two different concepts of privatization' (1986) 46 *Public Administration Review* 285, 285.

6 Kolderie, ibid 285.

7 See, eg, A Acharya, *Targeting Terrorist Financing: International Cooperation and New Regimes* (New York: Routledge, 2012).

8 See, eg, W Jennings, 'Governing the games: high politics, risk and mega-events' (2013) 11 *Political Studies Review* 2; M N MacDonald and D Hunter, 'The discourse of Olympic security: London 2012' (2013) 24 *Discourse and Society* 66.

(3) above).[9] As contemporary counter-terrorism is essentially an exercise oriented towards the provision and production of the public good of security, the use of privatization across these three dimensions as part of counter-terrorism is something by which we ought perhaps not to be surprised. That this privatization would take place also in the context of surveillance – to which we shortly turn in a more sustained manner – is indicated by the hyper-connected nature of the modern world in which the networked realities of open and easy to access technologies such as the internet and cell phones create security risks and realities that states might most efficiently tackle by means of the involvement of private actors.

Building on these general observations about the concept and nature of privatization, this chapter classifies privatization in the counter-terrorist context across four different types. These are not unique to surveillance but rather reflect the broader phenomenon of privatized counter-terrorism. First, 'open' privatization by means of out-sourcing grounded in open contracts, which are declared and can be subjected to public critique and analysis. Secondly, 'closed' privatization by means of out-sourcing grounded in closed contracts, where the existence of either the out-sourcing relationship or the content of the contract is not disclosed and is not subject to public critique and analysis. The frequency with which these kinds of contracts arise is not known, but we do know that they exist in at least some counter-terrorist contexts such as for logistics support in extraordinary rendition.[10] Thirdly, statutory privatization,

---

[9] See, eg, F B Hare, 'Private sector contributions to national cyber security: a preliminary analysis' (2009) 6 *Journal of Homeland Security and Emergency Management* 7.

[10] See, eg, F de Londras, 'Privatized sovereign performance: regulating in the 'gap' between security and rights?' (2011) 38 *Journal of Law and Society* 96.

where legislative obligations are placed on non-state actors to engage in relatively specific activities that feed into broader state-run counter-terrorist strategies and policies. Placing asset freezing obligations on banks is a common example of this in the counter-terrorist context. Fourthly, non-contractual co-option, where non-state actors are 'co-opted' into counter-terrorism in an informal, networked manner without any clear outline of the parameters of the co-option or, indeed, publicization of the fact of the co-operation, co-option and counter-terrorist activities of the non-state actor involved. The original arrangement between the Society for Worldwide Interbank Financial Telecommunication (SWIFT) and American intelligence agencies relating to transaction tracking is a well-known example of this.[11]

This chapter will not examine open and legislative privatization in any detail. This is not to suggest that these types of privatization are not sites of concern, but in recognition of the fact that – from a constitutionalist perspective – they are of relatively less concern than are closed privatization and non-contractual co-option. Open privatization raises a low level of constitutionalist concern because the existence and general content of the contract is known and can be challenged. Not only is the information required to challenge open privatization publicly available but rights-related structures applicable to the content and processes of such privatization exist. It is clear that under international human rights law states have an obligation to take into account their international obligations in the crafting of privatization

[11] P M Connorton, 'Tracking terrorist finance through SWIFT: when US subpoenas and foreign privacy law collide' (2007) 76 *Fordham Law Review* 283.

decisions and contracts.[12] Furthermore, in domestic law there will often be some mechanism in place by which 'private' actors undertaking work on behalf of the state can be held to account in an analogous manner to governmental actors. Section 6 of the Human Rights Act 1998 (UK) and the constitutional state action doctrine in the United States (US) spring immediately to mind.[13]

Statutory privatization is also relatively unproblematic from a constitutionalist perspective. This is because the statutes in question will be subject to the same constitutionalist limitations on legitimate statutory activity as is all legislation. Thus, for example, the mere fact of privatization might be challenged as an unlawful delegation of state authority, the content of the privatized obligation might be subjected to scrutiny for compliance with constitutional or statutory human rights guarantees, and some mechanism of accountability (whether judicial, administrative of parliamentary) is likely to be built into the overall legislative framework.

This is not to suggest that these mechanisms of privatization are *entirely* unproblematic; rather that they are relatively less problematic than closed and non-contractual co-option. This chapter will concentrate on the latter only. Non-contractual co-option can be frequently observed in the context of counter-terrorist surveillance. It is not clear to what extent, if any, closed privatization arises in this context.

---

[12] K de Feyter and F Gómez Isa, 'Privatisation and human rights: an overview' in K de Feyter and F Gómez Isa (eds), *Privatisation and Human Rights in an Age of Globalisation* (Antwerp: Intersentia, 2005) 1, 3.

[13] The latter is discussed in D Barak-Erez, 'A state action doctrine for an age of privatization' (1994) 45 *Syracuse Law Review* 1169.

3 SURVEILLANCE: COUNTER-TERRORISM EVERYWHERE

PCTS is an exercise by the state in harnessing immense amounts of privately owned and developed technological awareness and capacity and using that technology to do, through or with the assistance of private actors, what is traditionally done by the state, that is, to survey individual actors' movements and activities for security-related purposes. By harnessing this private capacity, the state can undertake counter-terrorist surveillance without either clearly adhering to the normal legal limitations to which the state is subject and/or without us being wholly aware of the extent to which our interactions with prima facie private actors, and in apparently private spaces, constitute proxy interactions with the state and in the public.

A relatively brief sketch of the extent of PCTS illustrates how the state can and does conduct counter-terrorist surveillance 'everywhere' by means of this privatization. The enormous private surveillance infrastructure that now exists includes both technologies that are expressly or manifestly concerned with surveillance and those which have surveillance capacity. These encompass a range of technologies from Closed Circuit Television systems (CCTV), to mobile phone and Global Positioning Systems (GPS) location capacities and internet search engines (all of which have counter-terrorist surveillance potential).

CCTV systems are incredibly prevalent both inside and outside commercial and private premises. They make the concept of going about one's business in some kind of privacy almost impossible to realise. Footage recorded on these cameras – for

which there is rarely any kind of permit required – can be and regularly is appropriated by states for multiple purposes: traffic control, crime control, investigation and so on. Identification through the use of CCTV footage can be remarkably swift and easy, especially if the state in question happens to have an extensive photographic database. A recent trend whereby police forces place photographs taken through CCTV cameras on social media sites, such as Twitter and Facebook, and seek 'leads' on identifying the individuals featured in these photographs adds a further layer of privatization to the use of CCTV and, indeed, the privatization of security and surveillance more generally.

Mobile phones also carry enormous surveillance potential. Making a phone call, sending a text message, or checking your email on your phone can allow for your exact location (or at least the exact location of the mobile phone in question) at that particular time to be identified and for this then to be fed into investigative and surveillance processes. In some newer phones, including the iPhone, 'location' settings that allow for the careless among us to identify where our phone is when it is lost or mislaid also allow for it to be traced when it is not, and even when no use is being made of the phone. The location information can be acquired by the state from the mobile phone operator, often through satisfying a far lower test than would be the case if that state wanted to survey us itself. Again, we are not always aware of the degree to which our everyday engagement with technology – 'checking in' on Facebook, using GPS on the phone to measure the length and average pace of our morning run, sending a quick text message to tell a loved one that we have arrived safely at our destination – opens the opportunity for the state to perform its sovereignty on us through the engagement of private actors. That sovereign

performance is invisible, at least until it becomes corporeally written upon us perhaps by being charged with a criminal offence or placed at the scene of a crime. The banality of it – the commonplace nature of our use of technology and the high penetration of mobile phones into even the most remote markets – makes it virtually invisible to those of us not specifically 'tuned in' to these kinds of uses of technology.

In the context of mobile phone and internet technology, we see very clear patterns of co-option of private or non-governmental actors in the context of counter-terrorist surveillance not only in terms of location data but also in terms of helping the state to monitor people's phone and internet usage without formal contractual or statutory agreements or obligations to do so. This is aptly illustrated by the so called 'President's Surveillance Programme' (the Programme) in the US. The Programme involved numerous telecommunications carriers both intercepting and disclosing to the government enormous amounts of information about contemporaneous telecommunications as well as telecommunications records.[14] This went well beyond the publicly disclosed interception of communications into and out of the US where there was a reasonable basis for concluding that at least one of the communicating parties was involved in or associated with terrorist organisations.[15] The exact scope of the involvement of telecommunications firms in the Programme is not conclusively known as the US Supreme Court denied *certiorari* in a suit relating to same.[16] But

---

14 See Inspectors General of the Department of Defense, Department of Justice, Central Intelligence Agency, National Security Agency and Director of National Intelligence, *Unclassified Report on the President's Surveillance Program*' (2009) <http://www.fas.org/irp/eprint/psp.pdf> (accessed February 2013).

15 Inspectors General, ibid 1.

16 *Hepting v AT&T Corporation* (Sup Ct, No 11-1200, 9 October 2012).

there is no doubt that communications were intercepted and diverted and communication histories handed over to the government by private entities in a massive surveillance operation without the knowledge of the individuals who were subjected to it.

The enormity and accessibility of the internet makes it a technology of great interest and utility to criminals generally and to terrorist organisations in particular. It can be manipulated towards such nefarious ends as recruiting potential terrorists, propagandizing terrorist activities and messages, communication (both specific and general), fund raising and cyber-terrorism. States are and have long been concerned with the capacity of the internet to offer a large and sophisticated platform for terrorist activity. The very nature of the internet – as a trans-jurisdictional phenomenon and technology – makes it difficult to control. Internet-related counter-terrorism is complex because it cuts across all three categories of internet governance issues as defined by Dutton and Peltu: internet centric issues, internet-user centric issues, and non-internet centric issues.[17] The first set of issues relates to the maintenance of efficient and reliable internet and requires, among other things, high adaptation capacity so that the internet can maintain functionality even while technology and other changes are impacting upon it. The second relates more specifically to internet-user behaviours particularly where the internet is 'misused', that is, used for illegal and/or 'inappropriate' activity. The third highlights the relationship between internet governance and broader socio-political concerns and policy areas. In the counter-terrorist context, we are concerned with, for example, the security of internet

[17] W H Dutton and M Peltu, 'The emerging internet governance mosaic: connecting the pieces' (2007) 12 *Information Polity* 63.

infrastructure from cyber-attack (internet centric), the use of websites and online fora to recruit potential terrorists (internet-user centric) and the mechanisms by which the internet connects (constructively and destructively) with broader politico-legal counter-terrorist infrastructure (non-internet-centric). In relation to all of these, some kind of engagement between state and non-state actors in internet surveillance can be discerned.

In trying to regulate the internet for counter-terrorist purposes, states are performing sovereignty: they are extending their power extra-jurisdictionally and infringing on individual liberties for the purposes of expressing their supremacy over terrorist organisations in the online terrain. Doing this involves states in trying to achieve a number of things including, but not limited, to 'seeing' suspect communications, tracking browsing histories and patterns, using geo-location technology to identify the location of particular users and removing material that is considered to glorify terrorism. These may be pursued through surveillance activities with which – as internet users – we might not be particularly comfortable, such as using keystroke technology to record every keystroke on a particular machine in order to 'read' written communications and record passwords. Other activities undertaken as part of counter-terrorist internet governance implicate governments in data mining and profiling processes that have high discriminatory potential, for example, recording the education, communications, financial affairs, medical history, travel, immigration, transportation and housing affairs undertaken online. Once more, we see here the non-contractual co-option of private actors in counter-terrorism by the 'nudging' of ISPs, major search engine operators and other online entities to record and report information about people's online activities. A few examples might be Google's

willingness to hand information about search and browser histories over to the authorities, agreement by search engines to either remove certain sites from their results or to privilege other sites when particular terms are used, and agreements by ISPs to filter out certain kinds of sites and content and, indeed, to remove content, including that which is identified as glorifying terrorism.

We are often entirely unaware of the extent to which our online lives are surveyed and made available as matters of public record when requested by states; statutes permitting for states to acquire information on online data are far from rare[18] and governments frequently moot more;[19] even where such statutes exist, they are sometimes circumvented by surveillance done without lawful authority or the cooperative handing over of data by private companies such as the notorious warrantless wiretap programme in the United States. Thus, internet service providers, search engines, social networking sites and other organizations have been co-opted into the state's counter-terrorist activities (because they are used to track our activity or because they hand information to governments) and we have all become subjects of counter-terrorism without necessarily perceiving our subjectivity in this way. This is not only part of what Simon Chesterman has documented as a new social contract with the surveillance state,[20] but also an example of pervasive privatization in the counter-terrorism context with serious constitutionalist implications.

[18] These statutes include express permissions for interference with online privacy (e.g. 18 USC Chapter 119: Wire and Electronic Communications Interception and Interception of Oral Communications) and national security exemptions from data protection laws (e.g. the exemption for intelligence and defence intelligence agencies in Australia's Privacy Act 1988 (s. 7(2)(a), Privacy Act 1988).

[19] In 2012 the UK government proposed the creation of what became known as a "snooper's charter" in the Draft Communications Data Bill (see further J Petley, "Panic Stations: Surveillance in the UK" (2012) 42 *Index on Censorship* 70) and as outlined by MacDonald in this volume intrusive measures have also been proposed in Canada CROSS REF.

[20] Chesterman, above n 1.

4 CONSTITUTIONALIST IMPLICATIONS OF 'PRIVATE' COUNTER-TERRORIST SURVEILLANCE

PCTS has at least two serious implications for constitutionalism, where constitutionalism is considered in a textured sense as a commitment to power being limited, transparent and accountable and where that commitment is given effect by legal, constitutional and organizational structures within the state. Across all three of these parameters – limitation of power, transparency in the exercise of power, and accountability for the exercise of power – PCTS is problematic. Although considered separately below, it is important to note that limitation, transparency and accountability are closely connected constitutionalist concepts. This is because the transparency of the exercise of power creates the impetus towards explaining that exercise and the possibility of being judged and held accountable for what is considered to be an unacceptable exercise of power. Those judgments become the mechanisms by which we outline the limits on the exercise of power.

4.1 Limitation of Power

It is trite to observe that our organization into politico-legal entities known as states represents a handing over by 'the people' of some power to the state to coerce and regulate our activity. This does not, however, mean that we hand absolute power to the state. Rather, we agree – whether conceptualized through the classical 'social contract' lens or not – that the state may exercise power over us within what we have defined as acceptable limits. In states that embrace legal constitutionalism, those

limits are commonly clearly delineated in written constitutions which, in turn, are enforced by courts. In states that embrace political constitutionalism, the limits may be less clear and more difficult to identify but, at a minimum, they reside in the common law civil liberties and the principles of natural justice expressed in judicial review. In both cases, it is clear that power is not *unlimited*. This is so even in classically political constitutions such as that found in the United Kingdom (UK).[21]

It is a core element of constitutionalism that the state will not act beyond those agreed limitations. To do so – to infringe upon our fundamental liberties by means of such extension – would be to rupture fundamentally the bond between the people and the state and call into question the legitimacy of the state's exercise of power. In this respect, of course, legitimacy must be unhitched from the concept of legality for this to be a matter of particularly serious concern. A wholly legalistic conceptualization of legitimacy may result in one having less constitutionalist discomfort with such applications of power provided they were pursuant to laws promulgated in a procedurally correct manner or an alleged executive power exercisable without any such legislative measure.

Surveillance by the state infringes on numerous of our freedoms, particularly expression, association and privacy.[22] However, when the state engages directly in acts of surveillance it must do so within agreed limits − procedural and substantive –

[21] See, eg, *R v Jackson* [2006] 1 AC 262. Lord Steyn, Lord Hope and Baroness Hale also suggested that there may be some limitations upon parliamentary sovereignty. This must be contrasted, of course, with the orthodox account of the political constitution in the United Kingdom: J A G Griffith, 'The political constitution' (1979) 42 *Modern Law Review* 1.

[22] Consider cross-referencing here to the chapter by Amos.

that delineate acceptable and unacceptable interferences with these freedoms. The same is not true of private entities, with which we do not have any kind of comparable 'bargain'. Indeed, we arguably give to these entities large amounts of our privacy and personal freedoms by our use of their services and agreement to their terms and conditions. Thus, these private entities may be empowered to infringe to a greater extent than states on our freedoms by gathering information about users. States manage, by means of non-contractual co-option, to 'piggy-back' on that infringement and benefit from it by receiving and processing the extensive information thus gathered. This may not constitute a 'hard' expansion of state power beyond the agreed limits (inasmuch as the state is not directly exercising the surveillance power). But, by any account, it is a de facto interference with personal liberties outside of those accepted limitations and is thus of constitutionalist concern.

4.2 Transparent Exercise of Power

It is not only fundamental that states would limit their exercises of power to accepted limits but also that such power would be transparently exercised. This does not mean – as, indeed, it realistically could not mean, given practical considerations – that the state must be absolutely transparent and open about every individual exercise of power upon an individual. It is, of course, the case that individual surveillance patterns and decisions must remain confidential for security reasons (although this does not preclude ex post facto disclosure and analysis). However, a constitutionalist commitment to transparency requires the disclosure of patterns of state surveillance which are all too often missing in the context of PCTS. Thus, while we do not (and should not) expect the state to write to us individually and tell us that our email

correspondence is being read and fed into a data processing system for counter-terrorist reasons, it is legitimate for us to expect that the fact that the state has partnerships with private entities (such as CCTV operators, ISPs, Facebook and so on) would be disclosed to us. This is important for two reasons.

The first is that we are entitled to expect that we can appreciate the situations in which we are interacting with the state and allow knowledge of that interaction to regulate our behaviours. When we interact with an entity that is manifestly identified as the state – such as, for example, asking a uniformed police officer whether she has any hints or tips about how one might make a bomb – we are immediately aware of the fact that we are engaged with the state. In this example, the questioner should reasonably expect that the police would take an interest in his or her activities. However, would such an expectation exist if the person in question typed 'how to make a bomb' into a search engine rather than asking a police officer? Here, there is no clear expectation or indication that one's curiosity about such an activity would arouse state suspicions. It may well be that we would like to know when people are, in fact, seeking information of this kind; we might think it quite advisable that such a search term would trigger a reporting obligation on the part of the search engine provider to the state. However, this is not incompatible with saying that we expect to *know* when our activities invite (or potentially invite) the attention of the state, especially when our immediate interlocutor looks nothing like the state and everything like a corporate actor.

The second reason why transparency is important from a constitutionalist perspective is more theoretical. Adopting the Arendtian commitment to the public helps us to see

the constitutionalist value of transparency.[23] For Arendt, 'public' is that which is subject to the public gaze and, as a result, in relation to which there is an imperative for justification and a possibility of judgment. This, in turn, of course, ought to catalyze a reflective ex ante process where the justifiability of the activity is considered before it is undertaken. Ideally this would mean that power remains within agreed-upon limits.

PCTS is problematic from this perspective because its covert nature means that the fact that it is being done to us might not be known at the time or, indeed, ever. Concealment of coercive, counter-terrorist and regulatory activity is a matter of concern to the Arendtian because actions done beyond the public gaze are not open to judgement and are therefore not subject to the imperative for justification. That relationship – between the possibility of being judged and the attendant requirement of justification – is, in a way, a philosophical writing of the basic constitutionalist principle that power should be transparent, accountable and limited.

4.3 Accountability for the Exercise of Power

Accountability is a rightly lauded concept in the context of constitutionalism, and public law and organization more broadly. Although the concept of accountability is a complex one, for our purposes it is sufficient to subscribe broadly to Bovens' classical articulation of accountability as both a virtue and a mechanism.[24] As a virtue,

---

23 H Arendt, *The Human Condition* (Chicago: University of Chicago Press, 1998).

24 M Bovens, 'Two concepts of accountability: accountability as a virtue and as a mechanism' (2010) 33 *West European Politics* 946.

accountability encompasses the behavioural commitment to acting in a manner that accepts – if not embraces – the submission of one's actions to scrutiny, accepting that there are limits (either substantive or procedural) on the permissible exercise of power. As a mechanism, accountability describes the means by which an actor is required to give an account of her actions to a forum which has the capacity to put in place some kind of consequence (whether that be a sanction or not) for the misapplication or maladministration of power. Understood thus, it is clear that there is at least some connectivity between accountability as a virtue and accountability as a mechanism. That is, in the absence of a mechanism for 'making one accountable', one might question the incentives for 'acting accountably', particularly in a situation of particular strain such as a perceived or actual security crisis.

Accountability is lauded and valued because it is a key mechanism for ensuring that the bargain struck with the state (that it will exercise power only within the limits set for it as considered above) is adhered to. Furthermore, it is a largely successful means of ensuring transparency—or of acting in Arendt's public gaze—which brings with it the imperative for justification and the possibility of judgment already considered. Accountability thus improves governance, provides opportunities for public catharsis, and bolsters constitutionalism. The importance of accountability to constitutionalism is illustrated by the attention that states have historically paid to establishing mechanisms for its achievement. Open parliamentary processes (including committees and parliamentary inquiries), elections, judicial review, a free press, and structures of bureaucratic organization are all mechanisms designed to both incentivize accountable behavior in the first place and ensure the discovery of unacceptable behaviours.

PCTS challenges accountability because it involves entities not normally subject to our core accountability mechanisms in behaviours with clear constitutionalist and liberty implications but leaves them outside of accountability structures. Even where contracts of some kind are used to bring private actors into security activities, there are difficulties with establishing clear legal rationales for subjecting them to conventional accountability structures and mechanisms: [25] the contracting party remains *private* and thus not subject—in our conventional understanding—to the same accountability structures as public actors are. The law frequently allows the 'private' actor to simply be treated as a contracting party governed by contract law and not as what it is in PCTS contexts: a differently constructed manifestation of state power. If the arrangement passes a test for treatment as a proxy state actor—such as the state action test in the United States or the hybrid public authority test under s.6 of the Human Rights Act 1998 in the UK—public accountability systems can be imposed, but these are difficult to establish[26] and in numerous contexts contractual context has been determinative.[27] They can also be frustrated by the invocation of strong immunity claims such as state secrets, or indeed by judicial deference to the security context.

---

[25] See, eg, *Mohammed v Jeppeson Dataplan Inc* 614 F 3d 1070, 1075-6 (9th Cir 2010), denying certiorari, albeit in the context of logistics provision this case illustrates the capacity of the state to deploy state secrets to prevent discovery of such contracts.

[26] For a general discussion see D Barak-Erez, 'A state action doctrine for an age of privatization' (1994) 45 *Syracuse Law Review* 1169.

[27] For example *YL v Birmingham City Council* [2007] UKHL 27.

In the absence of any contractual nexus with the state – such as in the case of non-contractual co-option – accountability can be even more difficult to achieve. This is not least because of the apparent ease with which states can insulate these actors from a key legal accountability mechanism for private entities (liability) by blocking discovery through invocation of doctrines such as state secrets.[28] Although some accountability mechanisms beyond law can flow where the involvement of private actors is discovered (such as market-based accountability, inquiries or being required to appear before a parliamentary committee), these are likely to apply only on an ad hoc and somewhat haphazard basis. They are insufficiently systematic to act as an effective regulator of private entities' involvement in counter-terrorist surveillance or of states' use of PCTS.

5 LAW IS ALL WE NEED?

Seen in isolation, PCTS may not seem to be something to which we need give an inordinate amount of attention. After all, as infringements on liberties in the context of counter-terrorism go, it is, perhaps, not the matter of the most pressing concern. One might also imagine that a fairly comprehensive regulatory framework – either legal or voluntary – might be introduced that would remedy at least some of the constitutionalist concerns that are raised above. However, there is a need here to recognize PCTS as a microcosmic illustration of three contemporary trends. These trends converge in this context to establish that what is lacking is not law per se but rather a commitment to constitutionalism in contemporary counter-terrorism.

---

[28] *Mohammed v Jeppeson Dataplan Inc*, ibid; *Hepting v AT&T Corporation* (Sup Ct, No 11-1200, 9 October 2012).

The first of these trends is the emergence of a counter-terrorist state in which counter-terrorism and security have become a dominating grammar informing and shaping swathes of state activity, policy making, resource allocation and political debate. In spite of the fact that more than a decade has passed since the terrorist attacks of 11 September 2001, that day remains a significant moment on the US and international political landscapes. This is so in terms of both the reams of law and policy introduced at the national, transnational and international levels in response (direct or indirect) to the attacks and its status as a signal event recalled in politics and popular culture with almost ritualistic frequency when new repressive laws, policies and practices are under discussion. In many facets of the 'war on terrorism' that emerged in the wake of these attacks, a counter-constitutionalist turn has been evident in liberal democracies such as the US, Canada, the UK and Australia of which the growth and adoption of PCTS is only a part. The core constitutionalist commitment to limited, transparent and accountable power is increasingly made vulnerable by reference to necessity, extraordinariness, risk and the need for secrecy. These concepts act as barriers to deliberation and to constitutionalist caution, creating the politico-legal space within which states can and do undertake expansive and repressive counter-terrorist activities, including counter-terrorist surveillance, with seemingly minimal concern for the constitutionalist implications thereof not just in strict legal terms but also from a broader perspective of commitment to the core pillars of constitutionalist democracy.[29]

[29] Consider cross-referencing to the Gearty and MacDonnell chapters here.

That this would – to at least some extent – involve the state in privatizing some of its counter-terrorist work ought not, perhaps, to be surprising given the decades-long pattern of contracting out, privatizing and co-option that can be observed across a wide swathe of traditional state activity. The state has steadily been engaged in a Janus-faced evolution whereby it appears to shrink (by the delegating of tasks and powers to non-state actors) but functionally expands (by the executing of state policy and concerns by these non-state actors) and the counter-terrorist context has not escaped this trend. In all of its manifestations, this pattern raises constitutionalist concerns. This is no less true of PCTS in which the concerns relate both to the core commitments of constitutionalism outlined above and individual rights protection.[30]

It should be noted that even were the state not to utilize PCTS to the extent considered above, the breadth of surveillance activities undertaken in the name of counter-terrorism – not to mention their covertness – ought still to be a matter of concern. As is outlined throughout this volume, surveillance is ever-expanding. Driven by and driving technological advances that subject human behaviors to automated and algorithmic analyses which can have serious implications for individual liberty, surveillance as a contemporary activity raises profound questions about law's capacity to contend with such technological advances in a manner that effectively protects individual liberties and reinforces the state's bounded power.[31]

Placed in the febrile context of counter-terrorism these difficulties are exacerbated, but fundamentally – in this context as in others – they are manageable. Although a significant and difficult task, legal innovation to ensure that rules and frameworks can

30 Consider cross-referencing to the Amos chapter here.

31 Consider cross-referencing to the chapters by Kremer, Cole, and Fabbrini and Vermeulen.

be developed to manage surveillance techniques, even as they become more technologically sophisticated, is by no means beyond the ability of jurisprudes, legislators and courts. What is absent, rather, is the core commitment to constitutionalist principles that is required as a foundation for the development, adoption and implementation of those rules and frameworks.

The purpose of this chapter has not been to illustrate a phenomenon with which law cannot contend; by a combination of innovations in public (including constitutional), private (including contract and data protection) and administrative law the phenomenon of PCTS could easily be brought under legal control. However, this requires a recommitment to core constitutionalist principles of limited, transparent and accountable power that are systematically undermined by privatized counter-terrorist surveillance. It is that recommitment that has so far proved to be lacking.