8 Privacy, bulk collection and "operational utility"

Tom Sorell

The Snowden revelations in 2013 concerned the large-scale secret collection of normally private personal communications data for counter-terrorism purposes. Both the American NSA and the British GCHQ were implicated. It is widely believed that the privacy rights of large numbers of entirely innocent US and UK citizens were violated or at least significantly limited by bulk collection. In earlier work, I have expressed scepticism about privacy-based criticisms of bulk collection for counter-terrorism (Sorell 2018). But even if these criticisms are accepted, is bulk collection nonetheless legitimate *on balance* – because of its operational utility for the security services, and the overriding importance of the purposes that the security services serve? David Anderson's report of the Bulk Powers review in the United Kingdom suggests as much, provided bulk collection complies with strong legal safeguards (Anderson 2016).

I think it is hard to mount a uniformly compelling operational utility argument, because purposes other than counter-terrorism are pursued by the security services with the help of bulk collection. For example, the Intelligence Services Act 1994, section 1(2) says that apart from the interests of national security and the prevention and detection of serious crime, the Secret Intelligence Service may act "in the interests of the economic well-being of the United Kingdom". The phrase "interests of the economic well-being of the United Kingdom" is open to a disturbingly wide range of interpretations. It might be taken to include the cybersecurity interests of very large companies headquartered or merely located in the United Kingdom (PwC 2017; Zetter 2010), or intellectual property interests of UK companies that are targets of foreign government or foreign company espionage. Do these interests justify (morally justify) government acquisition and analysis of large personal data sets? In my view the answer to this question is "No", unless there is a clear and significant benefit to UK citizens in general from the cybersecurity of the large companies in question. Even when relevant "economic interests" are confined to those "also relevant to the interests of national security", as required by the Investigatory Powers Act (2016) section 204 (3a), the legitimacy of intelligence service action to promote or protect these interests is disputable. In particular, it is disputable when the action in question involves bulk collection.

DOI: 10.4324/9781003164197-12

For example, domestic manufacturers of weapons and military equipment are economically important to the United Kingdom and also important to UK security in some sense; it does not follow that intelligence services can legitimately act in the interests of those companies by directly supplying them commercially useful information obtained by bulk collection. Yet electronic interception for these purposes has taken place (Dover 2007), possibly assisted by acquisition of bulk personal data sets.

Other purposes that bulk collection serves include the recruitment by the United Kingdom of intelligence agents abroad. Is *this* purpose not at the very least morally ambiguous, given the mortal dangers faced by agents in some countries, and the moral dubiousness of treachery when agents are recruited to act against their own country's interests? The answer appears to be "Yes". Counter-terrorism and other purposes closely allied to life-saving are *differentially* compelling as grounds for bulk collection if bulk collection is effective. Counter-terrorism is unsurprisingly emphasized in the case studies favouring the use of bulk collection in the Bulk Powers report. But it is unclear what proportion of uses of bulk collection are for counter-terrorism, and so the utility of bulk collection may not have the justificatory power that Anderson's report implies it has.

The rest of this chapter falls into three parts. In the first, I go into some of the privacy objections to bulk collection, and why even some of the more sophisticated of these do not appear to me to engage with the mechanics of bulk collection. Then I consider the Anderson Bulk Powers report. It concedes that bulk collection is privacy-violating, but maintains that the right to privacy can be limited by the right to security, and that bulk collection can be effective for ensuring security, as illustrated by the case studies in his report. Since the purposes served in the case studies are not exhaustive of the purposes to which bulk collection is put, the question arises whether the remaining purposes legitimately limit personal privacy. If the answer is "No", there may be an argument for limiting the purpose of bulk collection to more or less uncontroversial security concerns, where being uncontroversial depends on probable prevention of large-scale injury or loss of life, rather than the pursuit of ill-defined "national economic advantage" or even strategic advantage. The subsequent sections deal with these remaining purposes. A final section draws conclusions.

Bulk Collection and Privacy

As I use the term, "bulk collection" refers to obtaining large personal data sets containing the information of, for the most part, entirely law-abiding persons. To illustrate, data sets composed of the names and addresses of bank account or credit card holders might be of interest to investigations of fraud or money-laundering or organized crime even if few people whose names are included have anything to do with those offences. Location data for people's telephones forms another relevant kind of data set, even if few of the telephones in question belong to persons of interest to the security services. In the same way, the names of passengers on airline flights between certain destinations might be collected, though

the majority of passengers concerned are travelling for entirely innocent reasons. Data concerning telephone or email exchanges is a further example.

After the Snowden disclosures, the bulk collection of communications data in the United States and the United Kingdom was widely condemned as a large-scale violation of the privacy of those whose data was collected (Shorrock 2013; Lyon 2014). The US legal understanding of *whose* privacy matters has changed since 2013, when Snowden first publicized the activities of the US National Security Agency. Before the disclosures, American law normally prohibited the collection of content from conversations between "US persons", but treated communications between foreigners or between US persons and foreigners, especially "agents of a foreign power", as fair game for purposes like counter-terrorism. In other words, the content of emails and other communications between US persons was normally out of bounds, but the content of emails and other communications between foreigners was not, if the purpose of collecting content was a legally recognized purpose of intelligence service activity. In the intermediate case of communications between US persons and foreigners, content collection was not necessarily ruled out, and might be permitted if the foreigners were employed by a foreign government. As for US persons' communications, although their *content* was normally out of bounds, their meta-data might be collected for purposes like counter-terrorism. Meta-data is information about email or telephone exchanges apart from their content. It might include the time an email arrived, the route it took through the internet to or from a particular IP address, how big the email was and what address it was sent to.

The American government's view before and even immediately after the Snowden disclosures was that US persons' communication data privacy matters more than the communication data privacy of foreigners, and that the collection of mere meta-data rather than content either does not rise to the threshold of a privacy violation at all, or at least counts as a relatively minor intrusion. After the passage of the USA FREEDOM Act in 2015, two things changed. First, bulk collection of US persons' meta-data was supposed to be discontinued. Second:

> the policy of the United States [was] that the privacy and civil liberties of everyone in the world must be taken into account when agencies collect signals intelligence.
>
> (Edgar 2017, 4)

In the United Kingdom, the Snowden disclosures also led to an official reconsideration of bulk collection by the intelligence services. David Anderson, a lawyer appointed as Independent Reviewer of Terrorism Legislation in the United Kingdom, issued influential reports successfully recommending law reform in the area of UK government access to communications data. These recommendations resulted in the Investigative Powers Act (2016), which introduced a regime of judicial oversight of warranting of targeted interception, bulk collection and "equipment interference" (hacking or malware installation). Anderson also conducted a review in 2016 of the actual security benefits of bulk collection, based on a mix of secret and publicly summarized case studies which the UK intelligence

services made available to him. This is the Bulk Powers Review that gives rise to this chapter.

The Conclusion of the Review concedes that bulk collection results in the storage and analysis without consent of large amounts of personal data. Under European law and international human rights treaties, this is an intrusion into privacy even if the data is not the content of messages, even if it is not "sensitive" or "protected" data to do with for example health, sexuality or religion, and even if it is not humanly inspected, but only held and processed by IT systems. The fact that bulk collection is invasive does not, however, mean it is impermissible. Anderson writes:

> international human rights instruments are pragmatic enough to recognise that intrusions into individual privacy will often be justified in the public interest. The privacy right may be overridden, where it is proportionate to do so, in the interests of national security, safety and the prevention of disorder or crime.
>
> (Anderson 2016, 119)

And, Anderson goes on, these are the interests promoted by bulk collection as used by the Intelligence services in the Review case studies.

> Each of the case studies is said to represent a success, small or large, against serious crime or threats to national security. They all involve intrusions, however technical, into the rights [to a private life and personal data]. But as they also illustrate, the benefits of successful operations are not simply measurable in a dry tally of operational gains. Individually and cumulatively, they change lives for the better.
>
> (Anderson 2016, 120)

At this point, several questions arise. First, granted that bulk collection violates a right to privacy, are the interests that it arguably serves weighty enough to override that right? Some of Anderson's illustrations – I come to them in a moment – might suggest the answer "No". Second, even if the interests that Anderson lists *are* overriding, do they exhaust the interests pursued by the intelligence services through bulk collection? Here the answer is a clear "No", since uses of bulk collection listed by the Intelligence services themselves for the Review include the pursuit of economic well-being and recruitment to MI6. These interests are *not* necessarily overriding, as I go on to argue.

A further question, and one that is perhaps more fundamental than the questions about overridingness just raised, can be put by asking whether privacy is satisfactorily understood in European or human rights law. In particular, it can be asked whether a loss of privacy or intrusion takes place when, as European law provides, someone loses *control* of his or her data (without consent) (De Hert 2008).

It is clear that one can lose control of information against one's will without losing privacy, as when one's diary is lost under a tonne of rubble after an earthquake. In this case, no loss of privacy has occurred because, though the diary is out of its

owner's control, it is not readily accessible to an interested reader. Even if it came to be in someone's control, say, because someone excavating the rubble comes across it, it does not divulge any information until someone actually reads the diary and takes in its contents. Until information is extracted and understood, there is no loss of privacy. But now suppose someone does read the diary. Even then it may be of no interest to the reader so that he or she disregards and forgets the diary's contents. If there is a loss of privacy at all, it is limited and temporary.

In view of cases like these, I favour a more restricted understanding of loss of privacy: namely when sensitive information – not just any old information – about someone (a) comes to the *attention* of someone else without the data subject's consent; (b) is grasped and remembered by that second person, and (c) the information is not normatively public. To take the last part of this formulation first, it seems clear that some information about oneself *ought* (morally ought) to be public – in the sense of being available for some time on the public record – whether one likes it or not – for example, the fact that a court has passed a sentence against one, or that one holds a public office, or that one has signed a petition, or that one is a qualified doctor. These are legitimately public pieces of information even though they are personal, because the institutions they are associated with are partly public-facing.

For example, the fact that someone has been sentenced to a crime should be on the public record because justice, as the saying goes, must not only be done but also be *seen* to be done. This is the effect of having public trial proceedings in due process-respecting jurisdictions, and records of verdicts and sentences. If the proceedings are normatively public, why is not a record of the proceedings normatively public? Again, certification bodies assure the public that identified people have the training to do certain potentially dangerous things, such as administering medical treatment, and where the certifications are missing, people should beware. Publicity in the case where certifications are missing or fraudulent is therefore obligatory. If it is discovered by an official or a patient that Smith is not a qualified or competent cosmetic surgeon, that fact needs to be made public, notwithstanding the fact that it is personal information about Smith. If a trial proceeds to a sentence before the eyes of anyone who wants to visit the public gallery of the court, then it is on the public record and ought to be available to members of the public who are not able to get into the public gallery.

Coming now to privacy and *attention*, it seems clear that this is what makes the difference between sensitive information being merely available for sharing and information actually being shared. Privacy is violated when availability of information turns into possession of information, that is, someone's taking in information intended not to be shared. Although mere availability facilitates possession of private information, it is not sufficient for loss of privacy, unless there is a reasonable probability that availability turns into possession. To return to the diary under a tonne of rubble, it is in some sense available to any excavator, but it is not likely to come into anyone's possession, because of the difficulty of excavation.

Finally, let us turn to sensitivity. Not every piece of personal information is sensitive. A person's shoe size or hair colour or the fact that they like chocolate ice

cream does not normally rise to the threshold for sensitivity, because there is no clear connection between that information coming into someone else's possession and probable loss of status or disadvantage or harm to the person the information concerns. Some kinds of information are conventionally protected against disclosure whether intended to be shared or not, because they so engage prurience, idle curiosity, prejudices, malice or other kinds of threats to the status of the data subject, that he or she should have the last word about disclosure.

In previous (sometimes joint) papers (Sorell 2018; Guelke and Sorell 2016), I have tried to give some indication of the range of sensitive information by reference to zones of privacy. These zones include the human body, the human mind (understood as the locus of one's fundamental beliefs and emotional attachments) and the home. Targeted surveillance using cameras, bugs and telephone taps penetrates many of these zones and is therefore often highly intrusive, as it gives surveillance agents access (visual or auditory) that is willingly extended by the surveillance target only to intimates, including access to unguarded expression of information that is not normally divulged to everyone. When cameras or taps or direct inspection are used, information normally classified as "sensitive" such as health information, or information about deep convictions, or about intimates, is extracted from secret observation of the body, secret listening in on people speaking their mind, or secret searches of a home. Again, targeted secret surveillance often bypasses triggers for voluntary concealment of one's body, or guarded or coded disclosure.

By contrast with targeted surveillance by means of bugs or taps, bulk collection does not necessarily penetrate the zones of body, mind or home. In particular, bulk collection of telephone meta-data – the staple of NSA work – is relatively unintrusive. It is not in itself a penetration of private zones, though it may lead to such a violation for example in a case where analytics of bulk collected data identifies someone as a suspect who merits targeted surveillance, say because he is in frequent email communication with a known jihadist.

Although bulk collection is not necessarily a privacy violation, other things are often wrong with it: for example, its secrecy (Sorell 2018; Lucas 2014), its eluding legal oversight and its supporting a far greater volume of searches and analyses than intelligence services are able to take in or act upon, so that it self-defeatingly produces acute information overload.

Doubts about bulk collection as a privacy violation are rarely heard from those writing on the ethics of intelligence.[1] But this may be because examples used by these writers are out of keeping with the way most bulk collection works. For example, Isaac Taylor writes:

> the privacy at stake when data collection is being carried out is what we can call informational privacy. The interest here is in not having certain pieces of personal information revealed to others under certain circumstances. Yet, even with this narrowing of the issue, the interest at stake is difficult to identify. I might have an interest in various people not having access to my medical records, but the reasons why I might want to keep those records private from one group of people (potential employers, say) might be very

> different from the reasons I want to keep them hidden from another group (like co-workers).
>
> (Taylor 2017, 329)

This passage makes it sound, first, as if bulk collection homes in on "sensitive" information, namely content from health or employment data bases, and as if this content might somehow come through bulk collection to the attention of people personally known to the data subjects (employers, co-workers) to whom they are sure they do not want to disclose this information. But this way of thinking misses the facts that (a) it is not nosey colleagues or bosses but machines with no human curiosity who are collecting the relevant data,[2] (b) counter-terrorism is the purpose of the collection, (c) connections with personal information depend on queries happening to excavate a name from a mountain of data and (d) meta-data rather than content is what has mainly been collected in cases emphasized post-Snowden: telephone meta-data at that. The latter point is worth making because a lot of personal communications meta-data, such as what number reaches a particular named person at a given address, has long been available in public telephone directories available to everyone – without anyone thinking that it is an invasion of privacy.

Operational Utility and Agent Recruitment

So far, I have argued that machine-collected communications meta-data is not particularly intrusive. Even if it were, its being useful for counter-terrorism would normally justify the invasion of privacy. I now consider uses of bulk collection by the intelligence services for purposes *other* than counter-terrorism. The Bulk Powers review report itself calls attention to the role that bulk collection by GCHQ plays in the identification of possible agents for recruitment as Secret Intelligence Service agents (Anderson 2016, 153). Again, the Intelligence Services Act 1994, section 2, authorizes activity by the SIS for pursuing the economic advantage of the United Kingdom. Are these uses of bulk collection unobjectionable? In this section I consider recruitment of foreign agents; in the next I turn to secret service action in the interest of national economic advantage.

The SIS in the United Kingdom recruits agents both at home and abroad.[3] Some recruitment is open and consists in part of inviting applications from university graduates, in much the way mainstream employers in the United Kingdom might. This form of recruitment would not normally require bulk collection, and there is reason to think that applicants who go through it get full information about the risks they run, as well as reasoned assessments of their aptitude for the work. In this way, both potential employees and the agencies decide to work together with their eyes open about what will be involved.

Matters stand differently where the agents to be recruited are from abroad and are identified, possibly with the aid of bulk collection, and approached secretly. There are good reasons why people should not (morally should not) act as secret agents for foreign powers, and these are also reasons why foreign powers should not try to recruit such agents, including with the help of bulk collection. Some

of these reasons are drawn from the moral character of the foreign powers doing the recruiting, and some are drawn from the character of the jurisdiction against whose interests a recruited agent would act.

If the power for which the prospective agent would operate is illiberal and undemocratic, perhaps even unapologetically authoritarian, then it has questionable domestic legitimacy; and the ground for its pursuing its own interests at the expense of another country's, still less another liberal democratic country's, seems weak. In a sense there is little reason for even a citizen of such a jurisdiction to promote its official interests abroad, since that country's official interests are often detached from those of its citizens. But, by the same token, there is even less reason for a foreigner to act against their own country's interests in the service of that sort of recruiting country's interests.

It is possible that agents do not see the interests they oppose or promote as strictly national ones, but instead as class interests or ideological interests with global constituencies. Perhaps agents for communist countries saw things this way in the closing stages of World War II and immediately afterwards. This does not make talk of betrayal of one's country or colleagues inappropriate. Kim Philby's information for the Russians compromised many UK agents. In particular, many of those sent to Eastern Europe were killed immediately after being deployed (Bethell 1994). Philby betrayed UK agents, and therefore in some sense the United Kingdom, even if Philby was setting out to advance the interests of an international proletariat.

So much for agents of illiberal powers, such as the former Soviet Union or Russia in our own day. There are further reasons why citizens or residents of liberal democratic countries should not be the agents of foreign powers – even if the foreign power is liberal and democratic itself. These are reasons drawn from the character of the agent's home jurisdiction. Quite apart from the existence of legitimate local laws against espionage – their legitimacy is by itself a reason for prospective agents to respect those laws – targets of recruitment in these jurisdictions benefit from local liberal democratic protections and probably enjoy economic opportunities for which they should be grateful. The minimal expression of such gratitude is to be law-abiding. Acting as an agent of a foreign power not only shows ingratitude: it also renders the agent an *adversary* of the local jurisdiction whose freedoms benefit him or her. The agent is rendered an adversary without necessarily having a grievance against that jurisdiction (he or she may simply want the money paid to an agent). So the betrayal can seem (morally) gratuitous. It can seem gratuitous even if the recruiting country has the same moral character as the local jurisdiction.

What about the recruitment of agents by liberal democratic countries from illiberal and undemocratic countries that systematically oppose the recruiting country? In particular, what are we to say about prospective agents who, while they are citizens or residents of a certain illiberal and undemocratic regime, deplore its illiberality and lack of democracy? In this case the citizens or residents may not benefit much from citizenship, and acting for the foreign power might contribute to the removal of a regime facing both domestic *and* foreign opposition for its illiberal and undemocratic ways. Here the case for internal resistance or even rebellion might

double as a case for accepting foreign assistance for a pro-democratic movement. Might it not also function as a justification for co-operation as an intelligence agent with a foreign power interested in, among other things, local democratization?

No. Intelligence agents respond to demands for information from a foreign jurisdiction. The foreign jurisdiction may itself be democratic, but *its* demos is not that of the agent's country. Its interests are not likely to be the same as those that would be pursued by a local demos after a regime change. So the idea that a local citizen interested in democratization might choose for that reason to become an intelligence agent for a foreign democracy seems ill-grounded. A person interested in democratization might look to external sources for funds, for example a would-be political party intending to operate in a democracy, but only by risking the impression of a party being directed from another jurisdiction. If, to avoid this impression, the money was secretly outsourced, that would undercut another norm of democracy – transparency – without cancelling the risk of undue foreign influence. In any case, if the choice of sources of funds were between an intelligence service and almost any other institution – an NGO, a private foundation, an international governmental organization – it is hard to see why the intelligence service would be preferred: it is too closely tied to the interests of a particular country rather than an interest in democratization. From many points of view, then, the promotion of liberal democracy does not seem to be an appropriate purpose of a foreign intelligence service, even the intelligence service of a democratic country.

The reasons for citizens of illiberal, non-democratic countries not to become agents of other country's intelligence services do not stop there. I have left out the obvious consideration that traitors in countries without due process are in mortal danger if discovered. They are likely to put not only themselves but also their families at risk. Even if their betrayal has been discovered, punished and officially acknowledged by all concerned through a public prisoner exchange and relocation to the country of their intelligence handlers, the agents are not necessarily safe, as the recent poisoning of Sergei Skripal by the KGB in Salisbury shows (Dejevsky 2019).

Even when the jurisdiction betrayed by an intelligence agent is sinister or worse, as in the case of Skripal, the fact remains that the agent is a traitor, and so is intelligibly an object of hatred of his countrymen and not only his country's officials. Especially where someone has acted enthusiastically as an intelligence agent for his own country before acting as an agent for another, the fact of his ending up in the pay of a human rights-respecting government does not confer on him much moral credit or put in a more favourable light his previous work for the illiberal government's intelligence service. In this respect, Skripal at his best was less estimable than a dissenter-turned-foreign-intelligence-agent.

Whether recruited at home or abroad; whether he or she acts for a liberal or an authoritarian regime, an agent accepts to lead a compartmentalized life, part secret, part open to his or her intimates. The role inevitably involves systematic deception of various audiences, some professionally hostile, others harmless, others positively supporting and loving. It also involves casually breaking confidences, and posing on demand as a holder of a variety of political views. David Cornwell

(AKA John Le Carré, the celebrated author of spy novels) was recruited while still a student at Oxford to work for MI5, and conscientiously infiltrated both left- and right-wing clubs. He was not above reporting the activities of close friends (Sisman 2015, chap. 6). This rather seedy behaviour appears only to have served the purpose of ingratiating himself with his handlers. The same casual betrayal of friends is associated with top-echelon spies. When Kim Philby's status as a Russian agent was conclusively established by MI6, he was not summarily arrested, but told privately in Beirut by an old friend and MI6 colleague, Nick Elliot, that the game was up (Macintyre 2015, chap. 14). This humane gesture was supposed to have led to a gentlemanly surrender by Philby after taking the opportunity of saying goodbye to his family. Instead, Philby promptly absconded and was next heard of in Moscow. Absconding was both a personal betrayal of the friend *and* an abandonment of his family, who were left with the shame of their relation to him and the embarrassment of being seen by others as possibly complicit.

Operational Utility and National Economic Advantage

I have been arguing that the use of bulk collection for prospective agent recruitment abroad is morally questionable, because prospective agent recruitment abroad is itself morally questionable. Agent recruitment from one's *own* citizenry for intelligence work abroad is morally justifiable, but it is presumably often possible *without* bulk collection. I now turn to a third purpose of bulk collection, namely pursuing national economic advantage. Unlike bulk collection for counter-terrorism or for the purpose of acting against serious and organized crime, bulk collection for national economic advantage is not readily connected to defence from life-threatening attack or even defence against other non-lethal harms, and it is notable that all of the bulk collection success stories presented to the Anderson review come from defensive activity.

In addition to its departure from self-defence, bulk collection for economic advantage seems to make countries who are otherwise military and intelligence allies into adversaries, at least temporarily. For example, France and the United Kingdom share intelligence about terrorists and people traffickers, but they have been, and will probably again be, competitors in procurement processes for military equipment in the Middle East and South Asia. In the context of competitive procurement, timely intelligence about discounts offered by France for large orders of military equipment are clearly of the utmost value to the United Kingdom (or UK companies bidding for contracts), and obtaining this intelligence is certainly within the remit of the SIS. Bulk acquisition has a role in identifying which officials in countries buying the equipment would have received price information, and which email accounts might therefore be worth penetrating. The same methods might also reveal who is in a position to be successfully bribed (SIS agents have exemptions from prosecutions under recent bribery law in England and Wales) (Horder 2011).

Espionage for economic advantage against competitors (as opposed to fully fledged adversaries) is a by-product of the end of the Cold War.[4] It takes at least two forms: the direct supply of intelligence information by a country's intelligence

services to firms from that country, and espionage in the service of the home government's economic policy. The second kind of activity might consist of equipment interference at laboratories or companies in a competitor nation. This sort of activity has relatively recently been agreed to be out of bounds by the G20, and by the United Kingdom in respect of China (Foreign & Commonwealth Office UK 2015). The first kind of activity has long been informally outlawed in the United States (Rascoff 2016), but not in the United Kingdom.

Dover documents a case in relation to UK arms manufacturers from around 2005. He highlights the process of a manufacturer's being introduced to foreign procurement officials by a local UK Defence Attaché, supported by a now defunct UK government body, the Defence Export Services Organization (DESO), and several intelligence services:

> Having received first indications marketing and been introduced to agents and procurement officials the manufacturer takes steps to provide them with a corporate presentation. Information on these officials and agents will have been collated locally by embassy officials *and might also have been subject to general or centralised information trawls by MI6, DIS and GCHQ* [my emphasis] – depending on the character and positioning of the person in question (interview 05IS; interview24IS; Scott, 1996, C2.26). These presentations are discreet and are held without publicity. The DA [Defence Attaché] will nearly always be in attendance at these presentations, as a representative of the UK government, and will often be in full dress uniform (interview 24IS). This emphasizes the UK government's backing of the product and also allows the DA to pass on convincing accounts of how the equipment has been successfully used by the UK's armed forces (interview 24IS; interview 18IS).
>
> (Dover 2007, 695)

A subsequent intervention might consist of an embassy reception held to underline UK government support for the proposed sale. At this stage, too, the intelligence services sometimes made a contribution:

> The primary motivation for hosting such an event is to give the manufacturers an overt 'kitemark' [mark of trust] of British government support. Such events also serve an information-gathering purpose – in soft terms as a means by which to network locally and illuminate matrices of influence and business. Of course, such 'soft' methods do not preclude the use of central intelligence assets – such as GCHQ to intercept communications or with human intelligence to reveal negotiating positions within rival companies or the client government, although this occurs only in a few notable cases (interview 05IS; interview 27IS).
>
> (Dover 2007, 696)

Dover does not emphasize *automated* evidence trawls; he is interested in "stovepiping" – the supply of intelligence – whether electronic or not, humanly

gathered or not – direct to officials of a company seeking a sale, as opposed to officials in government. His discussion nevertheless illustrates what sometimes happens when the intelligence services act "in the interests of the economic well-being of the United Kingdom".

Now for the central question: "What, if anything, is morally wrong with what Dover describes?" First, and most obviously, it is not immediately clear that promoting sales of a UK company always contributes much to the well-being of the United Kingdom as a whole. Whether it does depend on for example how much UK tax the company pays, how many UK citizens it employs and how well it pays them. Supporting a UK arms manufacturer raises further issues. For one thing, arms sales have traditionally been associated with corrupt payments of "commission" or other euphemistically labelled charges (Gilby 2014). Again, it matters what type of customer is buying. Is it a liberal democratic regime that is constrained in its resort to force? Or is it an authoritarian government that is not above using its weapons against its own or other civilians, for example in a proxy war? When these questions are pressed in the case of sales to Saudi Arabia – highly relevant at the time Dover carried out his research – it is not clear that moral justification for intelligence service assistance for arms deals is very strong if it exists at all.

It might be thought that while intelligence service pursuit of UK economic well-being in general is perhaps open to the criticisms made in the last paragraph, intelligence service pursuit of UK economic well-being through bulk collection is not, at least when it is lawful. Under the Investigatory Powers Act (2016) section 204 (3a), bulk collection for national economic well-being is permitted only where it is "also relevant to the interests of national security". Not every company seeking to sell goods or services in foreign procurement exercises will contribute to national economic well-being as well as having relevance to national security. So, clause 3a does seem to work in some cases to limit what the intelligence services can do. Unfortunately, this is not its effect in the problematic area of arms. Supporting big UK arms manufacturers is arguably always "relevant" to the interests of national security, in the sense that sales (even to dubious regimes) finance research that leads to innovation in military technology that undoubtedly helps to protect the United Kingdom. So, if the "relevance" clause was intended to limit economically motivated bulk collection to unproblematic cases, it does not seem to go far enough.

Perhaps the cases that the "relevance" clause most uncontroversially applies to are those in which the intelligence services assist in monitoring and responding to cyberattacks on UK companies. Here the purpose of bulk collection, for example of email meta-data for attack attribution, is defensive, and the beneficiaries are a very large range of organizations in both the public and private sectors of the United Kingdom. In the past, cyberattacks have been directed at UK communication companies with large customer bases as well as the National Health Service: in the latter case, the connection between preventing those attacks and increasing UK *economic* well-being is obscure. Other kinds of well-being are relevant instead. Protecting these seems more urgent morally than in the case where the interests of UK arms makers are assumed without argument to line up with UK interests.

The UK National Cyber Security Centre (NCSC) is a branch of GCHQ. As its 2019 Annual Report makes clear, it has developed a number of software tools for companies and public sector organizations to use in routine cybersecurity, and it has devised special safeguards for government networks that it is adapting for the NHS to prevent attacks like the WannaCry ransomware exploit in 2015 against the National Health Service. The NCSC Annual Report for 2019 gives examples of tools it has developed:

- the NCSC "Internet Weather Centre", which will aim to draw on multiple data sources to enable full understanding of the United Kingdom's digital landscape
- the Infrastructure Check service: a web-based tool to help public sector and critical national infrastructure providers scan their internet connected infrastructure for vulnerabilities
- Breach Check: a web-based tool to help government and private sector organizations check whether employee email addresses have been compromised in a data breach

(National Cyber Security Centre 2019)

At least the first of these three tools seems to involve bulk collection, and this time for cybersecurity and economic purposes that seem reasonable. The reason is that the tools are defensive, and are partly used to defend public institutions. The use of these or other tools to give the UK or UK companies is less strongly justified at first sight, because the question of who benefits from UK economic advantage and to what extent, needs to be specified first.

Conclusion

I have been arguing that the best case for the moral justifiability of bulk collection is where bulk collection clearly contributes to counter-terrorism. Anderson's claim that bulk collection of this kind is privacy-violating, but that privacy violations are a price worth paying for the prevention of terror attacks, concedes too much to privacy concerns. According to me, the simple collection and machine processing of personal information that never comes to personal attention, and that does not lead to targeted surveillance, is not by itself a privacy violation. The personal information of the average citizen in the United Kingdom, though held in data bases, is no more likely to receive attention than the diary under tons of rubble after an earthquake. It is simply too disconnected from the electronic travel, communication and financial transaction profiles of people who are reasonable targets. What is more, the information is not typically "sensitive" in senses I tried to elaborate in the first section. Typical personal information is protected not only by the law but also by judicial interventions in the authorization of bulk collection; it is also protected by the sheer amount of data and the sheer number of data analytics exercises that are needed to provide actionable intelligence.

Not every goal pursued by the UK intelligence services is as closely connected to the protection of lives as counter-terrorism. Agent recruitment is not. The pursuit of greater UK economic well-being is not. On the contrary, these purposes are arguably morally questionable in many cases. Foreign agent recruitment is an invitation to treason with all the attendant risks to the welfare and life of the agent and his or her family. The pursuit of UK economic well-being is conducted by the SIS under a regime that permits bribes and perhaps encourages "stove-piping" and the over-identification of state interests with the interests of economically important UK companies. Bulk collection in the service of these morally questionable purposes is itself morally questionable – whatever its operational utility.

Notes

1 An exception is Macnish (2018).
2 Of course, it is possible that people with access to data sets captured through bulk collection are personally interested in the addresses and financial records of particular people, but this fact is a reason for their not being employees of institutions that compile and analyze the data bases for counter-terrorism. It is not a reason for abolishing the data bases or for not building them in the first place. There have been cases of security service misuse of bulk data bases, including out of noseyness or simple convenience but no one suggests these are very numerous (Bowcott and Norton-Taylor 2016).
3 Not every intelligence service recruits foreign agents. The CSIS in Canada apparently does not.
4 See Porteous (1996; 1995).

References

Anderson, David. 2016. *Report of the Bulk Powers Review*. London: HMSO.

Bethell, Nicholas. 1994. "Profits and Losses of Treachery: Victims of Kim Philby's Betrayals Are". *The Independent*, September 6. www.independent.co.uk/voices/profits-and-losses-of-treachery-victims-of-kim-philbys-betrayals-are-staking-a-claim-to-the-cash-1447065.html.

Bowcott, Owen, and Richard Norton-Taylor. 2016. "UK Spy Agencies Have Collected Bulk Personal Data since 1990s, Files Show". *The Guardian*, April 20. www.theguardian.com/world/2016/apr/21/uk-spy-agencies-collected-bulk-personal-data-since-1990s.

De Hert, Paul. 2008. "Identity Management of E-ID, Privacy and Security in Europe: A Human Rights View". *Information Security Technical Report* 13 (2): 71–5. https://doi.org/10.1016/j.istr.2008.07.001.

Dejevsky, Mary. 2019. "Opinion: There Are Still Questions about the Skripal Poisoning That No One Wants to Answer". *The Independent*, 4 March. www.independent.co.uk/voices/skripal-poisoning-salisbury-attack-yulia-russia-novichok-putin-a8807191.html.

Dover, Robert. 2007. "For Queen and Company: The Role of Intelligence in the UK's Arms Trade". *Political Studies* 55 (4): 683–708. https://doi.org/10.1111/j.1467-9248.2007.00669.x.

Edgar, Timothy H. 2017. *Beyond Snowden: Privacy, Mass Surveillance, and the Struggle to Reform the NSA*. Washington, DC: Brookings Institution Press.

Foreign & Commonwealth Office UK. 2015. "UK-China Joint Statement 2015". *GOV.UK*, October 22. www.gov.uk/government/news/uk-china-joint-statement-2015.

Gilby, Nicholas. 2014. *Deception in High Places: A History of Bribery in Britain's Arms Trade*. Illustrated edition. London: Pluto Press.

Guelke, John, and Tom Sorell. 2016. "Violations of Privacy and Law: The Case of Stalking". *Law, Ethics and Philosophy* 2016 (4): 32–60.

Horder, Jeremy. 2011. "On Her Majesty's Commercial Service: Bribery, Public Officials and the UK Intelligence Services". *The Modern Law Review* 74 (6): 911–31.

Lucas, George R. 2014. "NSA Management Directive #424: Secrecy and Privacy in the Aftermath of Edward Snowden". *Ethics & International Affairs* 28 (1): 29–38. https://doi.org/10.1017/S0892679413000488.

Lyon, David. 2014. "Surveillance, Snowden, and Big Data: Capacities, Consequences, Critique". *Big Data & Society* 1 (2): 2053951714541861. https://doi.org/10.1177/2053951714541861.

Macintyre, Ben. 2015. *A Spy among Friends: Philby and the Great Betrayal*. London: Bloomsbury Paperbacks.

Macnish, Kevin. 2018. "Government Surveillance and Why Defining Privacy Matters in a Post-Snowden World". *Journal of Applied Philosophy* 35 (2): 417–32. https://doi.org/10.1111/japp.12219.

National Cyber Security Centre. 2019. *Annual Review 2019*. London: HMSO. www.ncsc.gov.uk/files/NCSC_Annual%20Review_2019%20FINAL%20double%20pages%20V2.pdf.

Porteous, Samuel D. 1995. "Economic/Commercial Interests and the World's Intelligence Services: A Canadian Perspective". *International Journal of Intelligence and Counter Intelligence* 8: 275–306.

———. 1996. "Looking Out for Economic Interests: An Increased Role for Intelligence". *Washington Quarterly* 19: 191–204.

PwC. 2017. *Operation Cloud Hopper*. PwC. www.pwc.co.uk/cyber-security/pdf/cloud-hopper-report-final-v4.pdf.

Rascoff, Samuel. 2016. "The Norm against Economic Espionage for the Benefit of Private Firms: Some Theoretical Reflections". *The University of Chicago Law Review* 83 (December): 249–69.

Shorrock, Tim. 2013. "A Modern-Day Stasi State". June 11. www.thenation.com/article/archive/modern-day-stasi-state/.

Sisman, Adam. 2015. *John Le Carré: The Biography*. 1st edition. London; Oxford; New York; New Delhi; Sydney: Bloomsbury Publishing.

Sorell, Tom. 2018. "Bulk Collection, Intrusion and Domination". In *Philosophy and Public Policy*, edited by Andrew I. Cohen, 39–60. London; New York: Rowman & Littlefield Publishers.

Taylor, Isaac. 2017. "Data Collection, Counterterrorism and the Right to Privacy". *Politics, Philosophy & Economics* 16 (3): 326–46. https://doi.org/10.1177/1470594X17715249.

Zetter, Kim. 2010. "Google Hack Attack Was Ultra Sophisticated, New Details Show". *Wired*, January 1. www.wired.com/2010/01/operation-aurora/.