Bulk Collection, Intrusion and Domination

Tom Sorell

Policing regularly involves surveillance. Informants pass on criminal plans to the authorities, and then it can be a matter for the police of watching and waiting near the place where the offence is supposed to be committed. Perhaps the suspects themselves will be watched and followed. Perhaps listening devices will be placed in their cars. These measures are not equally intrusive. Watching in public places is less of a violation of privacy than looking through the windows of homes, especially where the homes contain non-suspects in addition to suspects. Following is more intrusive than stationary observation at the scene of a supposed bank robbery or burglary. Unconcealed watching in public spaces is more easily justified than unpublicized watching, and so on.

What about technology-assisted surveillance? This is widespread and probably more common now in the developed world than surveillance conducted entirely by people. There is an extensive range of surveillance technologies, and differences between them can matter morally. Some technologies are more questionable than others, because they can intrude into the kinds of spaces that by convention are the most private. What is more, they can intrude into these spaces without the knowledge of the targets of surveillance. Other technologies are less intrusive but collect huge quantities of information very quickly. Sometimes the quantities can be disproportionately large. Again, over time, the information can be analysed for purposes quite different from those for which it was originally gathered, and some of these purposes are less easy to endorse morally than others.

For example, Automatic Number Plate Recognition (ANPR) can keep track of vehicles that are known to be uninsured or stolen or to be travelling in a zone attracting special financial charges, but it can also track the movements of particular people not suspected of any crime who are simply of interest personally to the operator of an ANPR camera or an analyst of ANPR data-bases. ANPR can also assist in terrorist investigations, although counterterrorism is probably not among the uses first envisaged for ANPR.

In 2013, Edward Snowden revealed the up to then secret use by the National Security Agency in the US of an intelligence-gathering program which incorporated several technological capabilities in combination: fiber-optic cable tapping, de-encryption, cyber attacks, telephone metadata collection, analysis and fusion, as well as bugging and tapping applied to the communications systems of governments friendly to the US. The system was designed for counterterrorism. Above all, it aimed at compiling an archive of communications data so complete that the task of finding a needle in a haystack –a previously unknown terrorist communicating with his terrorist associates—would at least not be hampered by the incompleteness of the haystack. The data came from the communications of US citizens with foreign nationals, and, in exceptional cases, from US citizens communicating with other US citizens. The form the data took was, roughly, records of connections between different telephone numbers at different times. When this data is aggregated, patterns of intensity of connection between different telephone numbers –some only indirectly connected— are revealed. Sometimes this called "contact chaining". Collection was supposed to proceed under warrants authorized by the Foreign Intelligence Surveillance Court, but sometimes, by the NSA's own admission, the terms of the warrants were violated.

NSA collection of telephone data was discontinued at the end of November, 2015 under the provisions of the USA Freedom Act, but some data already stored by the NSA, or by telecoms companies, is in principle still legally accessible by the NSA. Similar technology is employed in the UK by General Communications Headquarters (GCHQ), the Signals branch of the UK intelligence services. Bulk Collection, as this form of data-gathering is known, is likely to continue in the UK, though it has temporarily been derailed by a recent decision of the Investigative Powers Tribunal, which has ruled past UK bulk collection to be contrary to the Human Rights Act.

Bulk collection has been claimed to amount to intrusion on an epic scale, and to bring Western democracies down to the moral level of the Stasi state of the former East Germany. According to me, this sort of claim is quite incorrect. Bulk collection is *not* particularly intrusive and, as practiced in the US and UK, it is systematically and profoundly different from the intelligence collection techniques of the Stasi. The fact that it is relatively unintrusive, however, does not mean that there is nothing wrong with it. There *is* something wrong with bulk collection: namely, the difficulty of overseeing it in liberal democracies that allow a great deal of intelligence work –

perhaps too much--to be done in secret. Bulk collection also carries the usual risks associated with the encapsulation of risk profiles in algorithms: these are the moral risks of error and discrimination and the operational risk of information-overload.

The rest of the discussion is divided into five sections. In the first, technologies for targeted surveillance will be reviewed, along with the risks of unjustified intrusion they carry. I shall address the question *why* intrusion is normally morally wrong. This will involve me in discussing the value of privacy and the different zones protected by established informal conventions about privacy. Privacy in the relevant sense is associated with *access* to information rather than *control* of information. On the basis of the distinction between access and control, I give reasons in the second section for thinking that bulk collection is *not* as intrusive as better established technologies used for targeted surveillance. Section 3 distinguishes the NSA and bulk collection from the Stasi and its methods of intelligence collection, and rejects the claim that the two are relevantly similar. In section 4, I introduce a concept from republican theory –that of domination—to articulate a sound line of objection against bulk collection: namely that it contributes to "domination" on a modest scale, that is, a *potential* for infringing some citizens' negative liberty, if it is not, as it is not, effectively regulated and overseen. I end by suggesting that the main problem with bulk collection is that too much information surrounding it is classified, wrongly impeding the scrutiny of even security-cleared, democratically elected legislators.

Conventional technology for targeted surveillance and zones of privacy

Targeted surveillance in many jurisdictions is assisted by the following, far-from-new technology: bugging, telephone wiretapping, CCTV cameras, hidden cameras, and ANPR. Bugs are devices for listening undetected to conversations in private rooms or vehicles. Telephone tapping technology allows for listening to, and recording, conversations on landlines installed in private residences and businesses. CCTV cameras are often mounted in outdoor locations and record or transmit or record *and* transmit images of people and vehicles in their relatively near vicinity. CCTV cameras can be disguised and secretly operated, or can have their presence advertised in prominent public notices close to where they are taking pictures. ANPR operates in conjunction with cameras trained on car number plates. These, too, can operate openly or secretly, depending on the purpose of use.

Not all of these devices assist targeted surveillance: CCTV and ANPR often do not. But where they do, and are used as part of a police investigation or a piece of preventive policing in a liberal democracy, they commonly require official legal authorization. The need for authorization reflects the fact that targeted surveillance is intrusive and that citizens of liberal democracies normally have a right to privacy. A right to privacy is normally legally overridden when citizens are suspected of being involved in planning or carrying out a serious crime. A serious crime is an unlawful act that is intended to cause serious harm.[1]

In order to understand why surveillance, including technology-assisted surveillance, needs to meet a threshold of justification, we need to ask what is normally wrong with surveillance. Surveillance is objectionable where there is significant value in being unobserved. Being unobserved has value where observation is inhibiting, where it interferes with intimacy, or where it enables someone else to share one's experiences or get personal information about one for no good reason and without one's consent. Secret surveillance is worse than open surveillance because it opens the target of surveillance to unwitting, possibly humiliating, or otherwise damaging, self-exposure.

Open surveillance assists protective counter-measures and can in principle deter the commission of offences. Secret surveillance in conventionally very private places, such as bedrooms or toilets, lies at the extreme of *im*permissibility. For one thing, it is hard to think of any legitimate interest that the public or anyone individual has in overhearing or witnessing, still less recording, nudity, sex or defecation.

To explain the degrees of intrusiveness of surveillance, and therefore the different thresholds of justification that have to be reached to outweigh intrusiveness, it helps to distinguish between different zones conventionally protected from uninvited observation or from uninvited reporting. In previous work both of my own,[2] and jointly authored with John Guelke,[3] I have identified three such zones: the body, the mind and the home.

By 'the body' is meant primarily the exposed or naked human body. Conventions for covering the body and for not uncovering the body are also conventions against surveillance of the body. Voluntary exposure is an intimate act while surveillance, in particular secret surveillance, undercuts intimacy. Involuntary or unwitting exposure takes away control of the boundaries one sets even for intimates. Involuntary exposure not only seems to contribute to sexual vulnerability,

but gives away the presence of disease, disability, injury or mutilation that can put one under the power of an attacker, or that can occasion unjustified distaste or revulsion. Privacy conventions put the control of self-exposure in the hands of the self and limit the unwanted social effects of observation or reporting that prompt ostracizing revulsion or distaste.[4]

The home, for the purposes of this paper, is the default location occupied daily by a person when not otherwise active. It is the zone where people rest and sleep and expect to be safe when engaged in either. It is the zone to which someone returns at the end of their day or from which they set out to conduct their active life. The home in this preferred sense need not be made of bricks and mortar. Even the "homeless" can have a default location they return to and which they feel is familiar and relatively safe, say an urban doorway where they keep a sleeping bag. Again, someone whose life is divided between a flat and the office for roughly equal amounts of time might have two places with a claim to count as home. There can be temporary default locations, like hotel rooms or passenger aircraft or cars, and the conventions for not entering or inspecting the home uninvited can apply to the hotel room or one's airline seat.

The home is by convention the default location not only of individuals but couples and families, with further conventions governing which rooms are shared and when by different individuals. A home in the form of a house may have semi-public and altogether private rooms, connected with the exposure of the body in those rooms or with the forms that intimacy take.

The third and most important zone of privacy is the mind, understood as the set of capacities for arriving at what to believe and what to do. The mind is not, for our purposes, private in the sense –famously called into question by Wittgenstein--of being accessible only to the subject, or being the place where "what it is like" to experience something registers. It is *normatively* private, meaning that it is wrong to force people to disclose their thoughts or convictions or to think aloud in some substantial sense.[5] Especially in contexts where there is some strongly enforced political or religious orthodoxy, and expectations that each person will publicly proclaim adherence, the freedom to make one's own mind up privately –*without* thinking aloud and without declaring one's possibly unorthodox conclusions—comes into its own.

More generally, the mind is the arena where, by arriving at reasons for beliefs, or beliefs on the basis of reasoning, one *makes* those beliefs one's own. In the absence of the normative privacy of the mind people are likely to be mouthpieces for the views of their parents, religious or political leaders, or their class. The normatively private mind is also in some sense the *pre-eminent* zone of privacy, because it is by using its capacities that an adult in a liberal democratic society can determine the limits of exposure of the body and public access to the home. Normative mental privacy, in short, helps with the governance of other normatively private zones, but not the other way round.

If privacy is what one enjoys when experiential and informational access by others to one's body, home, beliefs and choices is significantly limited, then it is easy to see that privacy facilitates the exercise of autonomy. The normative privacy of the mind helps one to think and choose for oneself, but the public conventions licensing limited access to the home also facilitate the exercise of the capacity to choose and to believe for reasons. It is at home that one can be oneself and expose oneself most easily, and the home space therefore provides opportunities for trying on different views with one's friends and family before expressing them publicly.

The three zones of privacy help to define one's private life, but do not do so completely. What one does privately is not only what one does in private *zones*, but also, in liberal societies at least, what one does outside one's public *roles* of citizen, employee and so on, in one's own time. Private life in this sense can include travel at one's own expense, anything done to maintain or extend one's friendships, and, of course, romantic and family life.

How bulk collection is different

Against the background of the value of privacy, it is not hard to see why intrusion through targeted surveillance needs a justification. Watching someone for long periods, or eavesdropping, even when it is done openly, is a way of penetrating a zone or practice of private life without permission. It not only provides knowledge of what someone's habits and preferences are –what he is like—but also information helpful to a programme of influence or control, official or otherwise. For example, stalking often involves surveillance with a view to control, but stalkers do not include the state

or institutions at all, and they sometimes are much more successful in preoccupying the mind with anxiety and disabling choice, than state surveillance.[6]

Secret surveillance, especially were technology assists penetration of the target's home and exposure of the body, is particularly violating, because it is most likely to open someone's unexpressed thoughts, choices and strong attachments to inspection, with the usual safeguards of reticence and deception bypassed. Bugs secretly placed in the rooms of a home are particularly intrusive, because of the collateral damage of intrusion on untargeted associates or intimates of targets. There is no reason for the privacy of *these* people to be violated, even from the point of view of the observer of the targeted person who knows he is guilty of terrible crimes. Again, there is no reason to eavesdrop on the family or romantic life even of criminals, unless the family or partner is an associate in crime.

So much for secret surveillance of the private zones. At the other extreme, where surveillance technology operates publicly in public space, say a major road, it is still possible to violate privacy. ANPR does not discriminate between the number plates of stolen cars being used for a bullion robbery and the number plates of private cars lawfully being used for a bit of tourism. In the latter case, lawful activity outside a public role –private life—is recorded indiscriminately, in circumstances in which the agent has an interest in going about his business relaxed, and therefore unscruitinized. Not that we necessarily have here a serious violation of privacy, in the sense of unconsented to violation of conventions that define the very sensitive zones, but we have an incursion into legitimately private life nonetheless.

Bulk collection for the purpose of contact-chaining has some of the characteristics of ANPR and some of the characteristics of secret surveillance. Like ANPR, it involves matching identifying numbers associated with suspects to other data; unlike ANPR, bulk collection has often, in fact almost invariably, taken place secretly.

<Figure 1.1 near here>

Figure 1.1 shows the process of intercepting, collecting and storing data from a signal or signals (say one or many telephone calls from a number associated with particular telephone subscribers, or one or more uses of an internet search engine from a certain unique IP address). Meta data (usually identifying the transmitting and sending

machines) are extracted, filtered and stored. Authorized queries are then answered by searching or analyzing the data and the results disseminated to agents in the intelligence services. In some cases the storage of data is time-limited.

The signals may be derived from splitting an undersea cable carrying digital data, or it can be harvested some server or other data receptacle located in the US or another country. In some countries telecoms companies hold the relevant data and intelligence agents can apply for access to it. In the US, before the Snowden disclosures, the Foreign Intelligence Security Surveillance Act section 215 allowed this process to be carried out only on signals from targeted persons, say people who on the basis of human intelligence were thought to be members of certain foreign extremist organizations or agents of foreign governments. Special restrictions existed on making US persons targets, though if US persons communicated with suspect foreign persons even the content of their communications could in principle be legally intercepted.

The sole, legally recognized, purpose of the NSA's targeting persons, and intercepting, storing and analyzing their communications data before 2015 was counterterrorism. How does bulk collection of this kind work? Investigations of targets reveal "identifiers" e.g. telephone numbers or email addresses, of people whom the targets communicate with. The identifiers disclosed may in turn influence the choice of "discriminants" that are used in the collection process. For example, suppose that the email address spy@hotmail.com is found in the electronic contact book of someone about whom there is a reasonably articulated suspicion (RAS) that he is a security threat. Then a relevant discriminant for a search of stored data may be 'all identifiers communicating with spy@hotmail.com.' A less broad discriminant would be 'all identifiers from Sudan communicating with spy@hotmail.com.' The more general the discriminant, the more the data collected qualifies as "bulk." Beyond that, there is no categorical distinction between bulk and targeted collection.

An RAS target A may have many identifiers, some unknown to the authorities, and may communicate with others, including other RAS targets and unknown but dangerous people, through intermediaries. Suppose that A has, among other identifiers, the Twitter handle @rasTarget. Then 'communicates with @rasTarget' would not single out those with whom A communicates by means of intermediaries. To cater for these one must see whether there is anyone A communicates with, who, repeatedly, soon after receiving A's messages,

communicates with someone else . The relevant discriminants would thus pick up patterns of communication one "hop" away from A. NSA bulk collection can legally involve searches of communication networks two hops away from A, but before 2015 this came down from 3 hops. Although there are limits on what intelligence services can do with identifiers that are hops away from RAS target identifiers, one can see that bulk collection can quickly multiply identifiers of interest well away from anyone who is an RAS target. This can make bulk collection look indiscriminate and speculative–a "fishing expedition".

Figure 1.2 illustrates the networks of communication contacts that can be identified, starting from A. The diagram shows that A communicates heavily with B, that A and B have contact C and other unidentified contacts in common, who are therefore prima facie identifiers of interest, and there are several targets in pink among B's network that B may be passing A's communications to, if B is an intermediary. If B is an intermediary, he has a considerable number of contacts not shared with A that are only one hop away from A. Any of these could turn out to be an identifier of interest, as could identifiers of receivers of *their* communications.

<Figure 1.2 near here>

So far we have been considering discriminants tied to an RAS target identifier. But bulk collection can be geared to less specific discriminants, e.g. all telephone calls for a range of dates between numbers from a certain area code in an American state and a certain foreign international calling code, say the code for Syria. Again, bulk collection can involve tracking locations of huge numbers of mobile phones. In this way, bulk collection can seem to become untethered, or at least risk becoming untethered, from definite evidence against particular people of wrongdoing.

Again, bulk collection can be used in connection with the detection of the use of encryption by certain internet users. If it is assumed that only people up to no good, including terrorists, would encrypt their communications, is the investigation of identifiers associated with encryption a morally defensible strategy? We will return to this question shortly. First, let us ask whether anything has emerged so far to support the familiar complaint that bulk collection is intrusive, in fact spectacularly so.

It is possible to deny that bulk collection is seriously intrusive without denying that it is morally objectionable in other ways, and this is the approach I take. I deny

that bulk collection is particularly intrusive, but I do not deny that bulk collection may be error-prone, discriminatory, and carried out on a scale that is vastly disproportionate to its success in identifying terrorists in the USA. When conducted by the NSA, bulk collection was on a gargantuan scale. According to articles in the London *Guardian* and Washington *Post*, millions of telephone records daily were being collected daily in 2013 in the USA, and as many as 25 billion device-location records were harvested in April 2012 alone.[7]

Given the scale of bulk collection, the results have been meager. Only 64 ISIL related arrests were made in 2014-15,[8] an unknown proportion of which were based on bulk collection, and not all of these led to criminal prosecution. In the UK, evidence given to David Anderson, the Independent Reviewer of Terrorism Legislation, suggested that bulk collection was very useful for "target" discovery in a sense of "target" including seeds and RAS target. David Anderson was also told that bulk collection was the principal UK weapon in the discovery and response to cyber attacks.[9]

Even if the scale of bulk collection is disproportionate to its proven results in counter-terrorism, it may seem undeniable that bulk collection is *also* intrusive, since it is geared to identifiers that are often attached to real people, and identifying the people behind email addresses or telephone numbers is intrusive, especially if conducted on a big scale and on the identifiers of people with no connection to terrorism. After all, it might be said, "even if only meta data is associated with an identifier, a telephone record can reveal intense communication between people, which, if it were to come to light, could be very embarrassing or damaging without revealing the commission of a criminal offence. Meta-data might suggest the existence of an affair or some other, so far hidden, piece of behavior, say the use of phone sex lines or a gambling obsession that is played out on the internet.

These points are reasonable enough, but they suggest inferences that might be made by a nosey human investigator in a case where he has met and is curious about the suspects. Machine algorithms that identify communications links between identifiers differ from the nosey investigator in at least two ways. First they lack consciousness, human interests and curiosity, and second, they sift through huge data sets at very high speeds to find concealed links between identifiers, the kind that might reasonably be expected of terrorists trying to avoid detection by the authorities. It is true that intense communication between a terrorist suspect and someone who is

only connected to the suspect romantically or commercially might register in the output of a search, but unless that contact was a security official or someone connected to a likely terrorist target, it might command no more interest than the identifier of a popular pizza parlour.

Defenders of bulk collection have often tried to counter charges of gross intrusion by distinguishing, correctly it seems to me, between meta-data of telephone calls and their content, and between collection and inspection of data. It is one thing to collect telephone meta-data, including the dates, times and duration of telephone calls, and quite another thing to listen to telephone conversations or recordings of telephone conversations. Listening is certainly intrusive, even if the wrong of intrusion is outweighed by the ability to prevent mass murder when the conversation reveals plans for an imminent large-scale attack. But merely collecting records of telephone contacts is not necessarily intrusive, and if intrusive at all, it may be only mildly so.

One reason why this claim is sometimes resisted is because two different theories of privacy are used, respectively, by defenders and critics of bulk collection. According to one theory, keeping one's data private is a matter of being *in control* of that data. According to the other theory, data is private until its content actually comes to someone else's attention, no matter whether it is under the control of the data subject or data producer. Imagine some personal letters forever buried by an earthquake, but still legible if unearthed. The writer of the letters does not know where they are. They are out of his control. But tons of rock keep them from being read. Must there be a loss of privacy if the writer has lost the letters and it is in principle *possible* for the letters to be unearthed? I do not think we are forced to answer 'Yes'. It depends on whether the letters *are* read or are *likely* to be read. In the earthquake case, the probability of being unearthed and read is vanishingly small.

Specific documents in the secret archives of the intelligence services or an hour's telephone data on the servers of a telecoms company are not necessarily *more* likely to come to the attention of someone who can understand their significance than the letters under the earthquake rubble. This fact may be underlined by the enormous amount of telephone and other data already collected, the number of queries that are daily being processed, and the high probability of information overload where intelligence collection and analysis meets operational decision-making. Even if information of interest *is* isolated by collection and analysis, it may not come to the

attention of people who recognize its significance and are able to act on it, given how *much* information there is to sift through. This means sensitive information is doubly insulated –first by the mountain of data it lies beneath, and second by the information overload of those charged with going through it: overload may work to make analysts blind to important information and not register its significance when it is taken in by a human consciousness.

The theory that clear-headed attention rather than loss of control takes away privacy fits in with the NSA distinction between collection and inspection. Attention is a version of inspection. Until attention or inspection has been achieved, content remains unintruded upon. If merely being in a *position* to inspect was sufficient for intrusion, then, incredibly, a person holding but steadfastly refusing to read someone else's private diary would never be able to maintain the privacy of the diary's contents. It makes more sense to say that privacy is intact *until* attention is trained on the diary, and even then someone may miss its significance.

The distinction between collection and inspection seems compelling in other, uncontroversial cases. For example, suppose a university or school examination has just ended. The scripts are picked up from each desk and are put in a pile. If collection were *sufficient* for inspection, then piling up the scripts would take someone much further toward examining them than is credible. Every school or university teacher knows that reading and grading are a much longer (and often more painful) exercise than collecting scripts from students.

Leaving aside the collection/inspection distinction, how revealing would identifiers and links between them be if they *were* able to be inspected? An identifier like a telephone number or email address is not uniquely identifying, since it can be used by more than one person, and since the official telephone subscriber or email account holder may be tied to a false name. Again, email accounts can be used or entered illicitly by imposters, even when correct names are used. And of course, malware and the use of bots can enslave someone else's computer, showing it as the source of malicious or nuisance email traffic, even though the traffic flows without the owner's knowledge or consent. This means that identifiers can be more loosely connected to real people than might be thought. Consequently, the collection and linking of identifiers may tell one much less about the referents of the identifiers than is assumed.

Even when identifiers are as identifying as a name and address in the physical world, they are the most minimal contribution to intelligence. After all, the name of the occupant at a postal address is often made public by the occupant, for the benefit of the postman. So the mere fact that bulk collection starts with and links identifiers may be no more problematic than someone making a list of the names of the self-identified occupants of houses, indicating which occupants live closest to each. This information, too, may be freely and publicly available to any observer. In a targeted surveillance operation, knowledge of a name and address is a precondition, not a result, of surveillance, and would not begin to scratch the surface of a suspect or his activities. At the level of discovering and linking identifiers, then, bulk collection is no more intrusive than the *pre*-surveillance stage of many targeted surveillance operations.

It is true that bulk collection may reveal patterns of communication that might justify *targeted* surveillance assisted by highly intrusive technologies such as taps and bugs. But bulk collection does not by itself constitute such surveillance or by itself involve the associated levels of intrusion. Bulk collection is much more impersonal and the results of queries much more general than the recordings of targeted surveillance. Bulk collection identifies complex patterns of communication without uncovering the content of those communications. It is impersonal, because telephone numbers can be chained without disclosing whose numbers they are, or how many identifiers correspond to one person or organization. Again, bulk collection produces no experience of people identified, still less of zones protected by privacy conventions. It is much less intrusive than a secret camera in a bedroom conveying images of sex to a human camera operator.

The NSA state and the Stasi state

In an article written in 2013 for the American magazine, *The Nation,* Tim Shorrock writes of being shocked that private industrial companies acting as contractors for the NSA should have access to so much communications data of US private citizens. Booz Allen was Edward Snowdon's employer, for example. Shorrock claims:

> …tens of thousands of Americans working for private intelligence contractors have access to the personal information of millions of their fellow citizens,

> including their phone and e-mail communications as well Internet chats on Yahoo, Google and other ISPs. Combine this private army of contractors with the outlandishly huge federal intelligence bureaucracy, and the term Stasi—the East German secret police frequently invoked by Bill Binney—doesn't sound like an exaggeration. Except this is state surveillance plus capitalism: spying for profit.[10]

My own view is that comparisons with the Stasi are a *gross* exaggeration. Shorrock trades on Edward Snowdon's claim that as an individual working for a corporate contractor he had access to the emails and other data of many individuals. This is similar to the access that an ANPR operator has to location data for a particular driver he is personally interested in. This does not make the ANPR system a Stasi-state tool. The *personal* purposes of the rogue operator are neither here nor there when what is at issue is how the collection and inspection of data adds to state power –at least if rogue users are relatively few and far between.

In order to be analogous to the Stasi state, the NSA state would have to collect data for purposes similar to the Stasi state's purposes in collecting the information it collected. The purpose of the NSA system, when not perverted by rogue operators pursuing personal vendettas or personal curiosity, is counter-terrorism. The purpose of the Stasi state was the enforcement of a political orthodoxy and the identification of individuals who challenged that orthodoxy by behaving in ways that are perfectly legal in the West. These are completely different purposes. It is true that the NSA apparatus may be unfit for its purpose, as its meager results in prosecutions suggest. But this does not lower it to the moral depths of the Stasi state.

The disanalogy between the NSA apparatus and the Stasi state does not end there. If we concentrate on bulk collection as opposed to de-encryption and cable-splitting, it becomes very clear that the Stasi state characteristically depended on highly *personal* reporting by paid collaborators reporting on work colleagues, family members and friends. From 1960 to 1989 the East German government enlisted between 250,000 and 500,000 people as informants.[11] These people would have had, and communicated to the government, a lot of contextualized knowledge of surveillance targets—hugely intrusive information that the state would otherwise have had to reconstruct.

East German civil society, such as it was, was contaminated for at least 30 years by a pervasive system of spying that was very personal and highly vulnerable to spiteful or malicious reporting. Worse, the content of the information provided was itself highly personal, a kind of systematized gossip, but with damaging consequences for people gossiped about if they showed an interest in or sympathy with West Germany, Western Europe or the United States.

Bulk collection is far more impersonal. First, it is aimed at the disclosure of links with suspects who can then be eliminated. The designation of a suspect as a seed or target is evidence-based. It is officially expected that lots of links with seeds or targets are completely innocent (hence the metaphor of the needle in the haystack), and for the time that bulk collection was legal, there were court-imposed constraints on whose telephone data could be investigated, how indirect communications links could be, and how long the data could be held. The fact that ISIL-related arrests of all kinds in 2014-2015 amounted to under 70, and that these were not just based on NSA data, suggests that the US is far less willing to act on bulk collection than East Germany was willing to act on any intelligence, even malicious intelligence. And since life out of detention in East Germany was much more grim than pre-arrest life in the US, the comparison between the two regimes does not stand up to inspection.

Again, bulk collection is a big data exercise. Its point is to represent huge numbers of communications as networks of contacts. As already pointed out, the results of network analysis are not by themselves very informative, but can indicate focal points for further investigations, perhaps with a view eventually to a pattern of targeted surveillance that really will provide the details of a planned attack or key players in financing terrorist groups.

What really *is* wrong with bulk collection

Bulk collection can be objectionable even if it is relatively unintrusive. It can be objectionable because (i) its use over a long time succeeds in identifying few terrorists; (ii) its use of discriminants reflect stereotyping or is too sweeping; (iii) the number of hops it allows from direct communications with evidenced-based suspects potentially makes too many others persons of interest; (iv) it is hard to regulate legally; and (v) it is hard for democratic legislative bodies to hold those in charge of it accountable under those laws that do exist.

Bulk collection either satisfies each of these conditions or risks doing so. The connection with (i) has already been made: very few arrests have been made on the basis of bulk collection or human intelligence. To touch on (ii), discriminants can be too broad, at least in the first instance. (iii) is a related difficulty: if communication links can be very indirect, many people with no connection to terrorists but who have communicated with numbers also communicated with by terrorists, can be put under suspicion.

For example, a search of all phone conversations from a certain American area code to Pakistan or Somalia or Yemen in a given week or month may be too sweeping to yield proper targets for bulk collection, because US citizens have family in these countries and may be communicating with them for reasons completely unconnected to terrorism. Just as communicating with Yemen or Pakistan may be entirely innocent, so may being the next door neighbor of the two people guilty of the mass shooting in San Bernadino. So police or intelligence services need a reason for casting the net wide, and they need to identify relatively low thresholds for being of no interest for people caught in that net. Otherwise, being from Yemen or living next to a terrorist, or calling a number a terrorist also calls, is sufficient –objectionably sufficient-- for being of interest to the authorities, in which case police suspicion is distributed according to unfair and discriminatory criteria. This may have occurred in the single conviction by 2015 of someone in the US on the basis of bulk collection.[12] Targeting people for the use of encryption may be similarly discriminatory. WhatsApp is protected by encryption, for example, but millions of its users don't know or don't care about that, choosing it for communications because it is free of charge, even internationally.

The fact that there have been very few ISIL-related arrests in the US, and still fewer on the basis of bulk collection, suggests that however rough and ready discriminants are at the stage at which they are authorized for application to collected data, the results of their application—namely the revelation of a set of linked identifiers—is far from triggering the detention of anyone associated with those identifiers. It may not even trigger any sort of targeted surveillance involving communications content associated with those identifiers. This is where one of the differences from the Stasi state is highlighted. In the Stasi-case, there was a very low threshold for being of interest and many more opportunities for informants to allege links with subversives when no such links existed. On the other hand, there was a

very high threshold in the Stasi case for being considered of no further interest if an informant found someone a convenient target. In the NSA case, communications links are neither simply alleged, and nor is their existence considered incriminating by itself. The terrorist who orders lots of pizzas by telephone does not throw undue suspicion on a pizza parlour that everyone else telephones.

Let us define the NSA-state as the US government and law enforcement agencies informed by NSA analysis of data. Then there is a straightforward way of distinguishing the Stasi state from the NSA-state, and that is by reference to Philip Pettit's refinement of Isaiah Berlin's concept of negative political liberty.[13] Negative political liberty is a matter of not being impeded by authorities in acting on one's choices. But even in slave societies it can *happen* that people get to act on their own choices, say because a particular slave-owner is benign, or so preoccupied by other matters that he cannot spare the time to make slaves act on *his* choices. This is negative liberty by neglect --not genuine liberty-- since the prevailing power structure permits the slave-owner to behave oppressively whenever he likes.

Philip Pettit has coined the term 'domination' for this sort of case, i.e. where an agent in a power structure does not actually interfere with the choices of a local agent, but has the authority or ability to interfere. More specifically, A dominates B when:

- A can interfere,
- with impunity,
- in certain choices that B makes,

where what counts as interference is broad: it could be actual physical restraint, or direct, coercive threats, but might also consist in subtler forms of manipulation.[14]

In the NSA-state with bulk collection there is at the very least a risk of arrest if location or communications data happens to link a US citizen with a terrorist. If all that prevents this happening is information overload or bad publicity after the Snowdon revelations, then the NSA-state might be said to dominate, even if it does not actually interfere with the choices of, the would-be suspects thrown up by the bulk collection process.

The people dominated by the NSA-state are a tiny fraction of the American population, the rest of whom enjoy not only negative liberty but non-domination from

the NSA-state. The Stasi-state, on the other hand, took away the (negative) liberty of all of those it removed from employment or put in prison on the basis of informants' reports. It drastically reduced the negative liberty of everyone intimidated into not reading Western literature and prevented from travelling to the West or associating with Westerners. It drastically reduced negative liberty by limiting what people could legally say in public. Again, even where no negative liberty was directly taken away, the Stasi-state can plausibly be said to have dominated *everyone* in East Germany, even those in its ruling party, since not even party members were safe from suspicion of treachery or departures from orthodoxy. In short, East Germany is plausibly said to be the agent of total "domination" in Pettit's sense -- in a way the NSA-state *cannot* plausibly be said to be. More importantly, the Stasi-state is much more obviously guilty of interference described as the deprivation of negative liberty simply, not just domination.

Secrecy and the Tension with Democracy[15]

Democratic control of the use of mass telecommunications monitoring seems to be in tension with secrecy. Secrecy is difficult to reconcile with democratic control because activity of which a would-be controller is ignorant cannot be controlled by that agent. But much of the most invasive surveillance has to be carried out covertly if it is to be effective. If targeted surveillance like the use of audio bugging or phone tapping equipment is to be effective, the subjects of the surveillance cannot know it is going on. I accept the need for operational secrecy in relation to particular, targeted uses of surveillance. Getting access to private spaces being used to plan serious crime through the use of bugs or phone taps can only be effective if it is done covertly. This has a (reatively slight) cost in transparency, but the accountability required by democratic principle is still possible.

There is an important distinction, however, between norms of operational secrecy and norms of programme secrecy. For example, it is consistent with operational secrecy for some operational details to be made public, after the event. It is also possible for democratically elected and security-cleared representatives to be briefed in advance about an operation.

A key body in the US that ought to be well placed to conduct effective oversight is the Senate Intelligence Committee. This 15 member congressional body was established in the 1970s in the aftermath of another scandal caused by revelations of the NSA's and CIA's spying activities, including project SHAMROCK, a programme for intercepting telegraphic communications leaving or entering the United States.[16]. The Committee was set up after the Frank Church Committee investigations, also setting up the Foreign Intelligence Surveillance Court. Its mission is to conduct 'vigilant legislative oversight' of America's intelligence gathering agencies.

Membership of this committee is temporary and rotated. Eight of the 15 senators are majority and minority members on other relevant committees – Appropriations, Armed Services, Foreign Relations and Judiciary – and the other seven are made up of another four members of the majority and three of the minority. In principle this body should be well equipped to resolve the tension between the needs of security and the requirements of democracy. First, the fact that its membership is drawn from elected senators and that it contains representatives of both parties means that these men and women have a very strong claim to legitimacy. Senators have a stronger claim to representativeness than many MPs, because the party system in the US is so much more decentralized than that in the UK.

Congressional committees in general have far more resources to draw upon than their counterparts in the UK Parliament. They have formal powers to subpoena witnesses and call members of the executive to account for themselves. They are also far better resourced financially, and are able to employ teams of lawyers to scrutinize legislation or reports. However, the record of American congressional oversight of the NSA has been disappointing. And a large part of the explanation can be found in the secrecy of the programme, achieved through a combination of security classification and outright deception. Leaving aside the active efforts that have been made by intelligence services to resist oversight, it is also important to consider some of the constraints that interfere with the senators serving on this committee succeeding in the role.

The act of holding members of an agency to account is a skilled enterprise, and one that requires detailed understanding of how that agency operates. The potency of Congressional oversight to a large extent resides in the incisiveness of the questions it is able to ask, based on expertise in the areas they are overseeing. Where

is this expertise to come from? Amy Zegart[17] lists three different sources: first, the already existing knowledge that the senator brings to the role from their previous work; second, directly learning on the job; and third, making use of bodies such as the Government Accountability Office, the Congressional Budget Office or Congressional Research Service. However, she goes on to point out forces that weigh against all three of these sources of knowledge when it comes to the world of intelligence.

First, consider the likelihood of any particular senator having detailed knowledge of the workings of the intelligence services unaided. Senators seeking election benefit enormously from a detailed working knowledge of whatever industries are important to the senator's home district – these are the issues which are important to their voters, and the issues on which they are most inclined to select their preferred candidate. Homegrown knowledge from direct intelligence experience is highly unusual, as contrasted, for example, with experience of the armed services, so while nearly a third of the members of the armed services committee have direct experience of the military, only 2 members out of 535 Congressmen in the 111th congress had direct experience of an intelligence service.

Second, can Congressmen acquiring the relevant knowledge while on the job? Senators have a range of competing concerns, potential areas where they could pursue legislative improvement: why would they choose intelligence? Certainly they are unlikely to be rewarded for gaining such knowledge by their voters: intelligence policy ranks low on the lists of the priorities of voters, who are far more moved by local, domestic concerns. And learning the technical detail of the intelligence services is extremely time consuming: Zegart quotes former Senate Intelligence Committee chairman Bob Graham's estimate that 'learning the basics' usually takes up half of a member's eight-year term on the intelligence committee. Zegart also argues that interest groups in this area are much weaker than those in domestic policy, though she argues for this by categorising intelligence oversight as foreign rather than domestic policy. On this basis she points to the *Encyclopedia of Associations* listing of a mere 1,101 interest groups concerned with foreign policy out of 25,189 interest groups listed in total.

Again, voters who do have a strong concern with intelligence or foreign policy are likely to be dispersed over a wide area, because it is a national issue, whereas voters concerned overwhelmingly with particular domestic policies, like agriculture,

for example, are likely to be clustered in a particular area. Term limits compound the limitation in the ability of senators to build up expertise, but are the only way to fairly share out an unattractive duty with little use for reelection, so most senators spend less than four years on the committee, and the longest serving member had served for twelve years, as opposed to the 30 years of the Armed Services Committee. Add to all of that the effect of secrecy, which means the initial basis on which any expertise could be built is likely to be meagre. Secrecy also means that any actual good results which a senator might parade before an electorate are unlikely to be publicisable – although large amounts of public spending may be involved – estimated at $1.5 billion. A senator from Utah could hardly boast of the building of the NSA data storage centre at camp Bluffdale in the way he might boast about the building of a bridge.

Secrecy also undermines one of the key weapons at Congress's disposal – control over the purse strings. Congressional committees divide the labour of oversight between authorization committees which engage in oversight of policy, and 12 House and Senate appropriations committees, which develop fiscal expertise to prevent uncontrolled government spending. This system, although compromised by the sophistication of professionalised lobbying, largely works as intended in the domestic arena, with authorisations committees able to effectively criticize programmes – publically – as offering poor value for money, and appropriations committees able to defund them.

In the world of Intelligence, on the other hand, secrecy diminishes the power of controlling spending. For a start, budget information is largely classified. For decades the executive would make no information available at all. Often only the top line figure on a programme's spending is declassified. Gaining access even to this information is challenging, as members of the intelligence authorisations and defense appropriations subcommittees can view these figures -- but only on site at a secure location – so that only about 50% actually do. The secrecy of the programmes and their cost makes it much harder for Congressmen to resist the will of the executive – the objections of one committee are not common knowledge in the way that the objections of the Agriculture committee would be.

The fact that so much of the detail of the programmes that members of the Intelligence Committee are voting on remains classified severely undermines the meaningfulness of their consent on behalf of the public. Take for example the 2008

vote taken by the Committee on the FISA amendments Act. This legislation curtailed the role of FISA itself. It reduced the requirement for FISA approval to the over-all system being used by the NSA, rather than needing to approve surveillance on a target by target basis. This Act also created the basis for the monitoring of phone and Internet content. However, very few of the Senators on the Committee had been fully briefed about the operation of the warrantless wiretapping programme, a point emphasized by Senator Feingold, one of the few who *had* been briefed. The other Senators would regret passing this legislation in the future, as information about the NSA's activities were declassified, he insisted. Whether or not he proves to be correct, it seems democratically unacceptable that pertinent information could remain inaccessible to the Senators charged with providing democratic oversight. The reasons for keeping the details of surveillance programmes secret from the public simply do not apply to Senators. Classification of information with the effect of blocking access by members of the Senate Intelligence Committee in particular seems unjustified if not simply perverse. This suggests the topic of a sequel to the current paper: the use of the classification system to impede oversight of national security.[18]

---

[1] For much more on what makes a crime serious, see my 'The Scope of Serious Crime and Preventive Policing', Tom Sorell, *Criminal Justice Ethics* 35 (2016): 163-82

[2] Tom Sorell, "Preventive Policing and European Counter-Terrorism." *Criminal Justice Ethics* 30 1 (2011):1-22

[3] John Guelke and Tom Sorell, "Violations of Privacy' and Law: the case of Stalking" *Law Ethics and Philosophy* (2017). John Guelke and Tom Sorell, "Liberal Democratic Regulation and Technological Advance" in *The Oxford Handbook in Law, Regulation and Technology,* ed. Roger Brownsword, (Oxford: Oxford University Press, 2017).

[4] Maybe there is something wrong with distaste full stop, whether ostracising or not. See Martha Nussbaum, *Hiding from Humanity: Disgust, Shame and the Law.* Princeton NJ: Princeton University Press, 2004.

[5] Thomas Nagel, "Concealment and Exposure" in *Concealment and Exposure and Other Essays*. (Oxford: Oxford University Press, 2002): 3-26.

[6] John Guelke and Tom Sorell, "Violations of Privacy' and Law: the case of Stalking" *Law Ethics and Philosophy* (2017).

[7] Glenn Greenwald, "NSA collecting phone records of millions of Verizon customers daily." Guardian, June 2013 https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order. How "How the NSA is Tracking People Right Now", Washington Post, https://www.washingtonpost.com/apps/g/page/world/how-the-nsa-is-tracking-people-right-now/634/

[8] Office of Intelligence and Analysis, "Analysis of ISIL-related arrests in the homeland from January 2014-September 2015" Unclassified Homeland Security document https://assets.documentcloud.org/documents/2515184/isil-related-arrests-in-homeland-from-jan2014.pdf

[9] David Anderson, *A Question Of Trust: Report of the Investigatory Powers Review*. (London: HMSO, 2015): 7.25

[10] Tim Shorrock, "A Modern-Day Stasi State" The Nation, June 11 2013, https://www.thenation.com/article/modern-day-stasi-state/

[11] For an account of the Stasi in the context of the collapse of the German Democratic Republic, see Edward N. Peterson, *The Secret Police and the Revolution.* Westport, CT: Greenwood Press, 2001.

[12] This may have happened to a San Diego resident of Somali origin called Basaaly Moalin, on the basis of records of money transfers whose beneficiaries were controversially thought to be terrorists: See the *New Yorker* article on his case: Mattathias Schwartz, "The Whole Haystack", The New Yorker, January 26, 2016. http://www.newyorker.com/magazine/2015/01/26/whole-haystack

[13] Isaiah Berlin, "Two Concepts of Liberty," in *Four Essays on Liberty*, Isaiah Berlin, London: Oxford University Press 2002.

[14] Phillip Pettit, 1996. 'Freedom as Antipower' *Ethics* 106 3 (1996): 576-604

[15] This section is adapted with significant revisions from John Guelke and Tom Sorell, "Liberal Democratic Regulation and Technological Advance" in *The Oxford Handbook in Law, Regulation and Technology,* ed. Roger Brownsword, (Oxford: Oxford University Press, 2017)

[16] James Bamford, *The Puzzle Palace: A Report on America's Most Secret Agency*, Boston: Houghton Mifflin,1982.

[17] Amy Zegart, "The Domestic Politics of Irrational Intelligence Oversight," *Political Science Quarterly* 126 1 (2011): 1–25.

[18] This is the message of someone with decades of experience in the US government of applying norms of secrecy. See J. William Leonard, "The Corrupting Influence of Secrecy on National Policy Decisions" in *Government Secrecy,* ed. S Maret and T Youn (Bingley: Emerald Publishing, 2011): 421-434. See also Sen Ron Wyden's comment on secrecy upon the reception of the 2012 report on the CIA interrogation Senate Committee on Intelligence, "Committee Study of the Central Intelligence Agency's Detention and Interrogation Program: Senator Wyden Additional Views" www.intelligence.senate.gov/sites/default/files/press/wyden.pdf#

Bibliography

David Anderson, *A Question Of Trust: Report of the Investigatory Powers Review.* London: HMSO, 2015. https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Web-Accessible1.pdf

James Bamford, *The Puzzle Palace: A Report on America's Most Secret Agency*, Boston: Houghton Mifflin,1982.

Isaiah Berlin, "Two Concepts of Liberty," in *Four Essays on Liberty*, Isaiah Berlin, London: Oxford University Press 2002.

Glenn Greenwald, "NSA collecting phone records of millions of Verizon customers daily." Guardian, June 2013 https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order

John Guelke and Tom Sorell, "Liberal Democratic Regulation and Technological Advance" in *The Oxford Handbook in Law, Regulation and Technology*, ed. Roger Brownsword, (Oxford: Oxford University Press, 2017)

John Guelke and Tom Sorell, "Violations of Privacy' and Law: the case of Stalking" *Law Ethics and Philosophy* (2017) https://www.researchgate.net/publication/316691730_Violations_of_Privacy_and_Law_The_Case_of_Stalking_1_Violations_of_Privacy_and_Law_The_Case_of_Stalking_33

How "How the NSA is Tracking People Right Now", Washington Post, https://www.washingtonpost.com/apps/g/page/world/how-the-nsa-is-tracking-people-right-now/634/

J. William Leonard, "The Corrupting Influence of Secrecy on National Policy Decisions" in *Government Secrecy*, ed. S Maret and T Youn (Bingley: Emerald Publishing, 2011): 421-434.

Thomas Nagel, "Concealment and Exposure" in *Concealment and Exposure and Other Essays*. (Oxford: Oxford University Press, 2002): 3-26.

Martha Nussbaum, *Hiding from Humanity: Disgust, Shame and the Law*. Princeton NJ: Princeton University Press, 2004.

Office of Intelligence and Analysis, "Analysis of ISIL-related arrests in the homeland from January 2014-September 2015" Unclassified Homeland Security document https://assets.documentcloud.org/documents/2515184/isil-related-arrests-in-homeland-from-jan2014.pdf

Edward N. Peterson, *The Secret Police and the Revolution.* Westport, CT: Greenwood Press, 2001.

Phillip Pettit, 1996. 'Freedom as Antipower' *Ethics* 106 3 (1996): 576-604

Mattathias Schwartz, “The Whole Haystack”, The New Yorker, January 26, 2016. http://www.newyorker.com/magazine/2015/01/26/whole-haystack
Senate Committee on Intelligence, “Committee Study of the Central Intelligence Agency’s Detention and Interrogation Program: Senator Wyden Additional Views” www.intelligence.senate.gov/sites/default/files/press/wyden.pdf#

Tim Shorrock, **“**A Modern-Day Stasi State” The Nation, June 11 2013, https://www.thenation.com/article/modern-day-stasi-state/

Tom Sorell, “Preventive Policing and European Counter-Terrorism.” *Criminal Justice Ethics* 30 1 (2011):1-22

Tom Sorell, “The Scope of Serious Crime and Preventive Policing.” *Criminal Justice Ethics* 35 (2016): 163-82

Amy Zegart, “The Domestic Politics of Irrational Intelligence Oversight,” *Political Science Quarterly* 126 1 (2011): 1–25.