Failure to collectively assess surveillance-oriented security technologies will inevitably lead to an absolute surveillance society

Timothy Mitchener-Nissen

University College London, UK. t.nissen@ucl.ac.uk

Abstract

The arguments presented by this paper are built on two underlying assertions. The first is that the assessment of surveillance measures often entails a judgement of whether any loss in privacy is legitimised by a justifiable increase in security. However one fundamental difference between privacy and security is that privacy has two attainable end-states (absolute privacy through to the absolute absence of privacy), whereas security has only one attainable end-state (while the absolute absence of security is attainable, absolute security is a desired yet unobtainable goal). The second assertion, which builds upon the first, holds that because absolute security is desirable new security interventions will continuously be developed each potentially trading a small measure of privacy for a small rise in security. When assessed individually each intervention may constitute a justifiable trade-off. However when combined together these interventions will ultimately reduce privacy to zero. To counter this outcome, when assessing the acceptability of any surveillance measure which impacts upon privacy (whether this constitutes a new technology or the novel application of existing technologies) we should do so by examining the combined effect of all surveillance measures currently employed within a society. This contrasts with the prevailing system whereby the impact of a new security technology is predominantly assessed on an individual basis by a subjective balancing of the security benefits of that technology against any reductions in concomitant rights, such as privacy and liberty. I contend that by continuing to focus on the effects of individual technologies over the combined effects of all surveillance technologies within a society, the likelihood of sleepwalking into (or indeed waking-up in) an absolute surveillance society moves from being a possible to the inevitable future.

1. Introduction

In 2004, Information Commissioner Richard Thomas¹ first warned that the United Kingdom was sleepwalking into a surveillance society,² before declaring two years later that ‘[t]oday I fear we are in fact waking up to a surveillance society that is all around us’ (Independent 2006).³ This statement implies that the rise of surveillance and corresponding fall in privacy represented a gradual culmination of events rather than a single conscious act. Privacy was suffering incremental erosion in the face of an equally incremental rise in surveillance, commonly justified by the need to enhance security. This resulted in an inevitable tipping-point whereby the surveillance society was realised. Now that this surveillance society

¹ UK Information Commissioner December 2002-June 2009; a post created as part of the UK’s efforts to fulfil its obligations under Article 28 of the EU Data Protection Directive (Directive 95/46/EC).
² A surveillance society is not solely characterised by physical monitoring through CCTV, but also by the collection and/or processing of communication, electronic, location, and personal data (Wood 2006), all of which impact upon our privacy.
³ This paper is written largely from a UK-centric perspective, reflected by the examples contained within. When I refer to ‘we’ or ‘a society’, I am referring to what I perceive to be the diverse multicultural morass that is the United Kingdom.

http://www.surveillance-and-society.org | ISSN: 1477-7487
©The author(s), 2014 | Licensed to the Surveillance Studies Network under a Creative Commons Attribution Non-Commercial No Derivatives license.
surrounds us it is readily recognisable, however trying to pin down the exact time of its genesis is an impossible task.

This paper is primarily concerned with privacy and the security technologies which have played a major role in expediting the UK’s surveillance society; hereafter referred to as surveillance-oriented security technologies (SOSTs). These are technologies intended to enhance the security of citizens via some inherent surveillance capability either operated by or accessible to the state. They facilitate the monitoring, screening, or threat assessment of individuals, groups, or situations, and are based on live-events, past events or the processing of data. In this paper I examine the prevailing assessment methods where the privacy impact of each of these technologies is predominantly examined on an individual basis; a common approach being the ubiquitous balancing metaphor whereby privacy reductions are legitimised by anticipated increases in security. It is my contention that by assessing the privacy implications of security interventions on an individual basis (as opposed to a collective basis incorporating all of the SOSTs operating within a society) the inevitable consequence is the realisation of a surveillance society. Privacy is ultimately extinguished as surveillance continuously expands until either attaining saturation or a maximal point determined by resource allocation, judicial complicity, political will, and/or technological ability; but always looking to expand where possible.

Before these arguments and their underlying assumptions can be developed, there are a number of fundamental topics which need to be addressed to provide the background and context for my arguments. This begins in section 2 with the definition and examination of privacy and security as they appear throughout this paper, a discussion of the reductionist approach adopted throughout, followed by a critical examination of the balancing metaphor. Section 3 identifies the different forces driving the development and implementation of new SOSTs, while section 4 examines the current security technology assessment methods which primarily treat individual technologies as discrete entities rather than as joined-up components operating together as a system. In section 5 I draw together these various discussions and set out my main thesis. Finally in section 6 I briefly begin to sketch out potential collective methods for assessing SOSTs when they operate concurrently. The goal of these methods is to protect privacy from becoming a collateral casualty in the unachievable quest for absolute security.

2. Privacy, Security, Reductionism, and the Balancing Metaphor

Privacy
Privacy is a concept so potentially expansive yet devoid of solidity that it led Solove to write ‘privacy seems to encompass everything, and therefore it appears to be nothing in itself’ (2009: 7). For the purpose of this paper I define privacy as ‘acting without being observed or recorded in any way’. This definition represents a non-normative, non-encompassing, quantifiable construction focused exclusively on the physicality aspects of the concept of privacy. The reductionist, individualistic construction adopted herein is markedly different from those more encompassing normative approaches for it does not engage with social aspects of privacy. Given the potential for controversy arising from such a definition, explanations and justifications for my definition follow below.

---

4 This definition is based on the work of Pavone and Degli Esposti (2010) who referred to SOSTs as the following devices: biometrics, biometric passports, CCTV, automated face recognition, automatic number plate recognition, passenger scanning, locating technologies, data retention, total information awareness, and eavesdropping. My definition is based on functionality and purpose; it includes all of Pavone and Degli Esposti’s identified devices but is not limited to them.

5 Also referred to as the trade-off approach.

6 This reflects Jeremy Waldron’s description of privacy as the condition of not being subjected to scrutiny which he adopts in an example relating to government monitoring of telephone conversations (Waldron 2003).
A non-normative definition: The academic discourse on privacy is vast and wide ranging as scholars attempt to distil the essence of privacy into encompassing definitions. Solove collated these approaches, categorising them into six general types: (1) the right to be let alone; (2) limited access to the self; (3) secrecy; (4) control over personal information; (5) personhood; and (6) intimacy (2009). These categories succinctly encapsulate and illustrate the diversity of mainstream privacy definitions. They range from definitions that seek to protect the individual from unwanted interference, such as the seminal right to be let alone (Warren and Brandeis 1890; Reilly and Cullen 2006), through to those that conceptualise privacy as a form of intimacy between people (Inness 1992). And just as norms within societies develop over time and new privacy-infringing technologies are introduced, so too do new definitions of privacy emerge. For example, the rise in centralised information collection and processing (facilitated by the concomitant rise in computers) inspired the emergence of information privacy. This was defined by Westin as ‘the claim of individuals, groups, or institutions to determine for themselves when, how and to what extent information about them is communicated to others’ (1967: 7), or more succinctly, ‘the ability to control information about oneself (Raul 2002: 1). The existence of these diverse conceptualisations, each seeking to approach privacy from a different angle, does not invalidate the competing approaches; it merely highlights the problem of defining privacy as identified by Solove. Similarly, my definition (which approaches privacy from the narrow perspective of physical privacy as it relates to surveillance) seeks only to add to this discourse. In the same way information privacy theories have added to (rather than challenged) the existing corpus of privacy discourse by focusing on a topical element, my definition merely seeks to complement existing theories rather than challenge their veracity.

A non-encompassing definition: A definition of privacy as ‘acting without being observed or recorded in any way’ represents an approach which is deliberately reductionist. Within my model I am only dealing with this single narrow aspect of privacy. Obviously this definition cannot be considered a comprehensive one, let alone anything approaching the scope of the taxonomy of privacy developed by Solove (2009).

A necessarily quantifiable definition: To balance privacy against security in the model proposed within this paper requires an empirical definition for privacy; one that will allow privacy to be transformed into a unit of measure. This would be impossible if I was to employ one of the broader normative definitions, especially those which emphasise social factors and subjective considerations. This need for objectivity is one of the identified challenges for any methodology which attempts to balance concepts which defy natural quantification.

A necessarily physical focus: The definition of privacy adopted herein complements existing broader definitions by focusing on the narrow aspect of physical privacy as it relates to surveillance. This important factor can be ignored or overlooked by broader definitions that focus on social interactions, personhood, personal data, and intimacy. A concern here is that physical privacy could be reduced to zero (thereby signifying an absolute surveillance society in the physical sense) while other aspects of privacy (such as communications, intimacy, social relations, medical data, etc.) are retained. For those who value their physical privacy, this scenario where other aspects of their privacy are retained may amount to poor consolation. Indeed it is arguable that these existing normative definitions have been unsuccessful in slowing or stopping the realisation of an absolute surveillance society forming within the UK as identified by Richard Thomas. Hence a physical-centric reductionist position is a necessary addition to complement and strengthen the overall conceptualisation of privacy.

Privacy under the definition adopted herein is considered a finite resource with two identifiable end-states and a quantifiable scale. At one end absolute (100 per cent) privacy exists when nobody has knowledge of

---

7 See the work of Loader and Walker (2007) as set out later in this section for more detail on this point.
your actions nor the capability to infer them, while at the other end the absolute absence (0 per cent) of privacy exists when all your actions are monitored. This reductionist conception of privacy can be reduced further into constituent elements such as physical privacy, geographical privacy, online privacy, etc. Thus one’s online privacy would represent the percentage of an individual’s internet use monitored either directly by the state or indirectly via internet service providers, including key-strokes, sites visited, and content accessed or downloaded.

It should be noted here that in asserting the existence of the end-state of absolute privacy I am making no claims as to how easy it is for an individual to attain this state. It may be as easy as closing a door to a room or removing the battery from a phone, or as onerous as hiding in a cave as far from populated areas as possible. This will all depend on a multitude of contextual factors.

**Security**

The concept of *security* has been appropriated and applied exponentially in the post-9/11 world. It has been interpreted to encompass everything from personal security, though to food security, transport security, infrastructure security, energy security, water security, viral security, online security, national security; the list is seemingly endless. Baldwin defined security as the ‘probability of damage to acquired values’ (1997: 13). He states that this definition:

> clearly includes the objective dimensions, and the subjective dimensions can be accommodated by designating ‘peace of mind’ or the ‘absence of fear’ as values that can be specified. Whether one wants to do this, of course, depends on the research task at hand.

(1997: 14)

In order to focus this discussion and develop an empirical model I have chosen not to include subjective dimensions. The *acquired value* being specified herein is *freedom from crime*. Security is therefore defined and measured as ‘the objective probability of being the subject of a crime’. I am not concerned with subjective notions (e.g. fear of crime, feelings of safety, etc.) or harms that are not crimes. I am however treating *crime* as the collation of all criminal offences within a jurisdiction rather than as a single specified act (e.g. assault or terrorism, etc.). Security is how likely the individual will be the victim of a crime from all possible criminal acts at any given time, including those which only arise in response to changes in policies, resources, technologies and capabilities. This reflects the fact that security is an endless quest where the end goal is a moving target as new attacks, challenges, and counter-measures expose new vulnerabilities and responses (Zedner 2005).

The requirements for the definition of security adopted herein mirror those of the privacy definition. It is a non-encompassing definition focusing on crime as a single aspect of security. It is a quantifiable definition in that it can be applied to countries where crime-rate data is kept, and it can be applied to an individual. Similar to the discussion of privacy, in adopting this objective definition I am not seeking to undermine the importance of subjective security, nor to disregard the often complex relationship between objective and subjective security. Rather I am simply focusing on its objective conceptualisation.

In contrast to the properties of privacy as outlined earlier, while security as defined herein also enjoys two finite end-states on a quantifiable scale, only one of these finite end-states is attainable: that being the absolute absence of security (0 per cent), readily conceivable as the moment an individual is the victim of a crime. Absolute (100 per cent) security is perpetually beyond reach (Baldwin 1997; Zedner 2005), leading to calls for the greater acceptance of insecurity (the inability to attain absolute security) as a natural part of the human condition (Neocleous 2007).

---

8 Within the UK incidents of crime are recorded by the police and disseminated by the Office for National Statistics.
A Reductionist Approach to Social Constructed Concepts

Both privacy and security are broad, socially-constructed concepts, each encompassing a multitude of constituent elements. My definitions for privacy (acting without being observed or recorded in any way) and security (the objective probability of being the subject of a crime) represent only two such elements. These definitions conceptualise an on-going real-world confliction between privacy and security that politicians and law enforcement officials continue to grapple with: that being how/whether to accommodate one’s right to act without being observed or recorded against the ever pressing need to reduce and prevent crime (be this property crimes, crimes against the person, terrorism offences, etc.). This reductionist approach of selecting a particular problem when dealing with privacy and security opens itself to criticism for not including the multitude of other elements which comprise privacy and security. However, narrowing the focus under examination does not disqualify this approach. It reflects the approach adopted by Solove in Understanding Privacy when identifying specific activities that create problems for balancing so as to improve processes (2009: see Ch.4). Indeed I would contend that this reductionist approach of focusing on specific problems and narrow aspects of security and privacy is a concrete, effective strategy for privacy discourse to influence decision making.

Another benefit of this reductionist approach is that it allows us to more easily quantify social constructs. In the model presented within this paper, security and privacy (both socially constructed concepts) are reduced and quantified with 0-1 scales, which is achieved by utilising the reductionist approach to identify and draw out two of the many specifiable objective elements which are themselves encapsulated by the much wider social constructs. This is not a unique idea: the concept of crime is a social construct, and yet we can reduce this down to specific offences and use arrest/prosecution data to engage in objective empirical analysis. For example, within an adequately run criminal justice system we can gather exact figures of how many people were charged with a specific offence over a specific time period which in turn can be compared over different time periods, thereby reducing these elements to numerical scales, despite the fact that the wider concept of crime itself is entirely socially constructed.

Balancing

Having defined both security and privacy I must address the balancing of these two social goods, an area which has been subjected to considerable academic discourse. The nature of balance implies the existence of values which oppose each other when both are engaged, whereby a measure of one may need to be sacrificed to promote the other for an optimal balance to be obtained (Loader and Walker 2007; Dragu 2011).

Despite the fact this balancing metaphor is employed by governments, state agencies, courts and the media, many critical thinkers have cautioned that when applied to security and liberty this metaphor is problematic. They warn it embodies a multitude of complex subsidiary factors which undermine both the plausibility of any bi-polar notion of balance, and it is highly questionable whether this metaphor can serve as an effective guide to practical decision making (Zedner 2005). Ashworth and Redmayne (2005: 40) caution that at worst balancing ‘is a substitute for principled argument: “achieving a balance” is put forward as if it were self-evidently a worthy and respectable goal, rather like “achieving justice”. Who, after all, would argue in favour of injustice or an unbalanced system?’

Waldron identifies reasons why we should carefully scrutinise the rhetoric of balancing. These include the resistance in civil liberties and rights discourse to consequentialism, the risk of an unequal distribution of liberty, and the unintended consequences of both reducing individual liberty and affording greater security powers to the state. There is also the risk of symbolic re-balancing, whereby those advocating increased security through decreased liberty cannot prove such actions will actually increase security (Waldron 2003).
Pavone and Degli Esposti (2010: 568) argue that while the trade-off (balancing) model seeks to oppose security against privacy by framing them as ‘exchangeable goods that [can] be traded’, this division is merely a symptom of the real issues for citizens which are trust and concern—the implication being that trust and concern are fluid, contextually-dependent attitudes based on personal and social factors, which cannot be traded like economic goods. Thus one can argue that privacy and security cannot be considered goods which can be traded, but rather socially embedded attitudes.

It has also been argued that security exists as a dynamic pursuit which makes balancing almost impossible as what lies in the scales changes every day (Zedner 2005), and that no one person can speak for all members of any society when deciding the trade-offs or balancing between different rights (Heymann 2001). Additionally there is the bold contention by Neocleous (2007) that the entire idea of balance between security and liberty is a liberal myth masking the fact that liberals prioritise security over liberty as evidenced by their propensity towards making authoritarian concessions to security. Balance, he claims, opens a back door route to the acceptance of authoritarian security measures and disguises the prioritisation of security over privacy. In a related vein, Dragu (2011) posits that by framing questions as to whether or not privacy interests outweigh security gains the debate is already tilted in favour of security. There is a presumption security should prevail, and the burden of proof is placed upon privacy advocates to prove the outweighing social value of their privacy rights.

Another problem with the framing of how privacy and security are to be balanced is that privacy is often portrayed as an individual’s right whereas security is a communal, societal right. Solove (2009) identifies that such a biased conceptualisation frequently leads to the value of privacy being outweighed; being forced as it is into a lopsided fight between the privacy rights of the individual against the security needs of the many. This conceptualisation ignores the social value of privacy. Raab (2012) has collated the various theories and approaches of those seeking to promote the social value of privacy. He writes that a greater understanding of the social benefits of privacy will create ‘a conceptual space in which privacy and the public interest could be understood in such a way as to enable both to be supported in many instances’ (2012: 130). It has also been claimed that rather than just serving the individual, privacy also fulfils societal needs and thus possess social value. Priscilla Regan, one of the theorists identified by Raab, posits that privacy possesses what she terms common, public, and collective values. Amongst other social benefits, it assists in the operation of a democracy by allowing citizens to cast votes without fear, and to promote freedom of speech and association; all examples of public values (Regan 1995). Hence the social, collective value of privacy should not be disregarded.

Finally there are the practical problems facing anybody attempting to engage in the empirical balancing of security and privacy in a manner which is neither arbitrary nor subjective, and is entirely based on the assumption that privacy and security are economically quantifiable goods—not least being:

- What value of unit should be assigned to each concept?
- Do these values increase and decrease at constant rates?
- Does the utility we assign to changes in each concept remain constant regardless of the level of security/liberty we both begin with and are left with?
- Does the nature and value of these goods remain constant during and after the act of balancing?
- And how many units of security are worth how many units of privacy?

As Loader and Walker state, the concept of balancing ‘lacks any clear, consistent and uncontroversial meta-rule or formula for resolving disputes between different values … [neither does it specify] how that comprehensive weighting is to take place’ (2007: 55).

Despite the multitude of reasoned arguments highlighting the weaknesses, inconsistencies, and flaws inherent to balancing, I believe we cannot nor should not reject this concept as a legitimate measure for
addressing conflicts between security and privacy. From a purely practical perspective there is the inescapable fact that balancing is deeply ingrained in the thinking, actions, and justifications of our entire political and judicial systems. As Zedner states, this balancing metaphor between security and liberty is so pervasive as to dominate legal and political debate, and this occurs despite its perilous nature and the doubt successive critical thinkers have cast on its usefulness or appropriateness (2005). To attempt to move away from balancing as the primary paradigm would meet such administrative, institutional and popular resistance that I am doubtful it would succeed. This state of affairs undermines the standpoint adopted by Pavone and Degli Esposti earlier which maintains that as privacy and security are socially embedded attitudes and not economic goods, they cannot be traded or balanced.

Furthermore, despite the extensive list of flaws set out in the discussion above, I believe we should actually embrace balancing when discussing surveillance because of the inherent strengths and benefits this concept brings with it. In relation to security and liberty, balancing forces the decision maker to acknowledge the existence, legitimacy and weight of those rights on the opposite side of the scales to security. Also, any legitimate act of balancing requires that the decision maker(s) engage in a chain of reasoning thereby exposing themselves to review and appeal by affected parties on the basis of, amongst other things; factors considered relevant, weights assigned, the decision making processes, and the final decisions taken.

However, the true threat associated with balancing is not the production of decisions based on a flawed, arbitrary, subjective process. The true threat is that decisions will be taken and technologies developed or deployed without balancing having ever been engaged in, thereby ignoring completely rights such as liberty and privacy. Consider the proposition by Zedner that ‘all talk of rebalancing presupposes a prior imbalance’ (2005: 511). While I sincerely wish this was the case, when discussing any confliction between security and privacy in the context of surveillance it is apparent that the presence of an imbalance is not a prerequisite for security advocates seeking to justify new SOSTs. Rather they can simply resort to basing their proposed measures on the risk of future crimes. Indeed it is debatable whether those who are focused on providing security or developing SOSTs ever conceptualise the presence of gaps in surveillance as presupposing an imbalance (and thereby being forced to assign a value to the opposing concept of privacy) or whether they merely see these gaps as threats that need to be addressed? If surveillance capability is perceived or framed as being desirable and good in-and-of-itself then the companies and individuals developing these technologies needn’t be concerned with ensuring privacy, rather they can simply justify their actions as focusing on maximising a desirable outcome. In this scenario there need never have been any imbalance (real or perceived) to begin with, for:

a) given the desirable nature of security;
b) the difficulty in promoting privacy as an equally desirable good; and

c) the commensurate ease with which security is promoted by those who prioritise this right,

an environment exists where surveillance technologies and techniques can be developed without any existing imbalance. It is an environment where the notion of privacy is afforded no balancing weight, assuming if it is afforded consideration at all.

Before moving on to discuss the forces driving the development of SOSTs in the next section, there are two final balancing points which need to be addressed. The first is a recurring claim by some commentators that, ‘[i]f personal safety is a necessary requirement for liberty, it must take priority in the relative ranking of these two goods’ and because security exists as a prerequisite for liberty we cannot therefore weigh one against the other (Meisels 2005: 164). While I agree that personal safety allows us to better enjoy other rights I strongly disagree with the resulting conclusion in regards to balancing. Where is the self-evident logical truth which requires us to move from accepting that security is a precondition to liberty to conclude that because of this fact we cannot engage in a balancing between these two goods? It
is an argument which, on a practical level, ignores the reality that governments, organisations, and individuals engage in this process (no matter how flawed or arbitrary) every day. On a theoretical level it is also open to challenge. To illustrate, assume one accepts the position that security is the paramount right of individuals (the provision of which is the most important duty of the state) on the basis that citizens need security to enjoy their other rights, including thought, association, privacy, etc. However, if security is promoted above all other rights, at the expense of these other rights, then eventually citizens lose both these other rights and their security, for they are now living in a totalitarian regime. It can also be argued that by losing their freedom they are no longer citizens. Hence what individuals and communities require to thrive as citizens with rights is for the state to provide a measure of security. Ideally this would be an amount which maximises the total quotient of all rights. To achieve this maximal amount requires the state engage in the very process of balancing rejected by Meisels.

Potentially Meisels’s argument would hold weight if security was a binary (all or nothing) concept while liberty existed on a dependent spectrum. An appropriate analogy here is that of a light switch with a dimmer attached; security represents the light switch and liberty the dimmer mechanism such that the dimmer can only work if the light switch is first turned on, thus enabling power to flow to the bulb. However, as Meisels herself acknowledges, both security and liberty are not all-or-nothing concepts (2005), and so I contend that as they both exist in degrees then at least the potential for balancing arises. Furthermore Schneier (2006) points out the fallacy of elevating security over privacy, highlighting that people living in open societies are more secure than those living in restricted countries where surveillance and restrictions on personal activities are pervasive. Those countries which place the greatest restrictions on the actions of state police are often those where the rule of law is most respected.

Secondly there is the fact that privacy and security are interrelated mutually reinforcing goods which need not necessarily exist in conflict (Dinh 2001; Dragu 2011; Raab 2012; Regan 1995; Roach 2006; Solove 2009), a fact which undermines the concept of balancing as some fait accompli. Security and privacy can be promoted in conjunction, for when we enjoy personal security it is easier for us to protect our own privacy, and vice versa privacy can enhance our security; it is hard to attack someone when you cannot find them. Similarly, security and privacy can be eroded simultaneously; collecting a wealth of intimate information on an individual for ostensibly legitimate purposes and storing it in a database will do little to protect either privacy or security if that information is stolen and used to commit identity fraud. Despite these arguments, the conceptualisation of security and privacy as inherently inversely-related remains the dominant paradigm used for shaping opinion, especially in antiterrorism policies where ‘reducing privacy protections is [seen as] necessary to reduce terrorism [and improve national security]’ (Dragu 2011: 74). It is coupled with the common belief that as security threats increase what is considered an appropriate and acceptable balance between privacy and security will change accordingly (Waldron 2003).

3. The Driving Forces Behind New SOST Interventions

New security technologies with surveillance goals are constantly being developed and implemented at a rate which appears to have grown exponentially since 9/11, and which shows little signs of abatement, from basic CCTV cameras to cameras as platforms for secondary technologies (e.g. biometric identification systems, automated threat detection algorithms, number plate recognition systems, etc.), GPS-enabled/device-centric tracking, to the digital universe of data-mining, data-matching, profiling, monitoring and tracking systems. What is clear is that this current frenzy of development has not arisen in a vacuum. There exists considerable pressure to both develop and maintain this pursuit of security given the political and financial capital already invested in it. Investors, industry, bureaucrats and elected politicians are motivated by strong personal interests (financial, political, ideological, etc.) to continue this drive towards an end-goal which can never be fully realised (Zedner 2005). Below I have sought to identify some of the driving forces behind new SOSTs:
Mitchener-Nissen: Failure to collectively assess surveillance-oriented security technologies

a. The intrinsic nature of absolute security: Attaining a state of security is a desirable end-goal, often referred to as the primary responsibility of governments, the paramount right of citizens, and a goal which legitimately justifies the sacrificing of competing rights. And yet absolute security is ultimately unobtainable regardless of the number of layers introduced; all security systems can be penetrated by attackers possessing sufficient resources, guile, and/or luck. Indeed each new security measure added to a system brings with it an associated cadre of new vulnerabilities for exploitation by a motivated attacker. It is the internal contradiction inherent to absolute security (being both desirable yet unobtainable) that acts as a self-justifying and motivational engine driving the creation of new SOSTs.

b. Fear and risk: Security products are marketed to prey on our darkest fears (Zedner 2005). This can result in four effects. Firstly it can create public demand for a solution to a (potentially previously unrealised) threat. Secondly, given that the state is always looking to limit the liberty of citizens, security threats such as terrorist attacks and other crimes provide excellent excuses and political coverage for the introduction of liberty-reducing measures (Waldron 2003; Neocleous 2007). Thirdly, by exploiting our fears of threats so as to justify new security interventions, the balancing voices of opponents will be muted for fear of appearing either unpatriotic (Waldron 2003), detached from the public, or simply lacking an understanding of the dangers of the real world. Fourthly there is the issue of risk language which is concerned with the probability of future events. According to Dinh (2001), terrorism requires us to act pre-emptively, neutralising threats before attacks are carried out. Statements like ‘we don’t know what the terrorists are going to do next so we must be prepared for anything’ create a convenient justification for the continuous design and implementation of new security technologies, without ever proving these threats are real. Additionally governments can deliberately encourage fear within citizenry to justify the introduction of new security technologies despite the absence of legitimate dangers. According to Pavone and Pereira (2009), these new technologies then facilitate more effective control and manipulation of citizens. By governments exaggerating threats and constructing a vision of society in which citizens are permanently depicted as targets of unpredictable security threats, individuals become more malleable, obedient, and open to self-sacrifice. ‘Inconveniently’, the effects of fear decrease over time so it becomes incumbent on governments to periodically reinforce (or reinvent) citizens’ feelings of fear, threat, and danger (Pavone and Pereira 2009). I would argue a recent example of such ‘fear-reinforcement’ within the UK was Prime Minister David Cameron’s claim that Britain is facing a generational struggle both home and abroad against Islamic terrorists.9 This reference to domestic security was made notwithstanding the absence of a successful Islamic-inspired terrorist attack within the UK in over five years. And the extraordinary long-term claim, that British citizens will be at war with such terrorists for a generation to come represents a reinvention of previous government fear discourse.

c. Political impetus: In recent years senior UK politicians have trumpeted the virtues of employing new security technologies to deal with security threats, from CCTV to whole body scanners, DNA databases to national identity cards. This is sentiment is also reflected at the European level (see European Commission 2004). In a 2008 speech on security and liberty delivered to the Institute for Public Policy Research, then UK Prime Minister Gordon Brown stated:

[the modern security challenge is defined by new and unprecedented threats: terrorism; global organised crime; organised drug trafficking and people trafficking. This is the new world in which government must work out how it best discharges its duty to protect people. New technology is giving us modern means by which we can discharge these duties.

---

When a Prime Minister is championing new security technologies as ‘the new 21st century means of detecting and preventing crime’ (Brown 2008), one should not underestimate both the legitimacy and momentum this endorsement affords such measures.

d. Pressure ‘on’ and ‘from’ police: Police forces are always under pressure to perform by both reducing crime and improving efficiencies and this pressure can be increased through the imposition of centralised targets, political posturing, and the direct election of chief officers. As such, the motivation exists for police forces to both adopt, and request, measures which help them achieve their targets. Reviewing the relevant strategy documents published by the Association of Chief Police Officers into technologies (including automatic number plate recognition, forensics, and CCTV usage) confirms that police view new SOSTs as an important means of achieving their goals.10

e. The availability of resources: The availability of funding for research and development (R&D) in a specific area is a great motivator for universities, researchers, and industry to enter that space, with security technologies proving a prime example. Within the Seventh Framework Programme of the European Community for research, technological development and demonstration activities (fp7), €1.4 billion was set aside specifically for security research (European Parliament 2006), which is itself separate to the national R&D security budgets of the 27 member states. In the United States, the Department of Defense’s basic R&D budget for 2011 totalled US$11.545 billion and the Department of Homeland Security’s science and technology R&D budget for 2011 totalled US$626 million (AAAS 2012).

f. Push from industry: One should never underestimate the power or effectiveness of the security industry to exploit past events and future threats to promote their own products, especially given that their business models and very survival depends on successfully selling their products. Given also that politicians want to be seen to be doing something in response to perceived threats, it is inevitable that a symbiotic relationship has grown up between politicians and the security industry. And it is an industry which is flourishing; as a simple example, the 2012 UK Counter Terror Expo had over 400 exhibiting companies alone.

g. Pull by the public: The UK public have generally been accepting of SOSTs, though with notable exceptions.11 Despite specific incidences of controversy, the public have supported the introduction of airport whole body scanners (Mitchener-Nissen, Bowers and Chetty 2011) and CCTV systems, where it is not uncommon for residents to lobby local councils to introduce cameras into town centres (see for example The Echo 2011; Derby Telegraph 2012).

4. Current individually-focused assessment methods

When focusing on privacy in determining the acceptability of a SOST, a number of methodological tools/procedures are available. The Human Rights Act 1998 (HRA) enshrines the European Convention of Human Rights (ECHR) into UK law, with Article 8 affording citizens the right to privacy and Section 6 placing a duty on public authorities to act in accordance with the Convention wherever possible. Additionally various countries have instigated privacy impact assessments (PIAs) to determine how privacy might be impacted by the development of a new technology (Wright et al. 2011). Public consultations may be undertaken to gather various stakeholder views when considering the deployment or

10 Unfortunately, given the impossibility of attaining absolute security under the model presented within this paper, neither increasing the number of new SOSTs nor improving their effectiveness will ever completely remove the risk of crime. So even if these new technologies are an improvement on traditional policing methods, the risk of crime will always remain and at some point privacy will become a collateral casualty as the quality and/or quantity of these technologies increases.
11 Namely national identity cards.
operation of new SOSTs. What links these different methods together is how balancing acts as an integral component of each and how the focus naturally falls upon the specific technology being examined.

In the case of human rights legislation such as the ECHR and HRA, privacy rights are not absolute. They can be interfered with when this is in accordance with the law and necessary in a democratic society for reasons including national security, the prevention of crime, and the protection of rights and freedoms of others. As Wright et al. (2011) state, the European Court of Human Rights (ECtHR) has also added a third criterion, proportionality, to these requirements. It is this along with necessity wherein balancing takes place. Additionally the ECtHR has traditionally refused to expand their balancing process beyond a weighing of two opposing values to a wider examination of the context in which these choices operate (Wright et al. 2011). The consequence when applied to the specific case of SOSTs is that individual technologies are not assessed collectively.

PIAs also employ balancing through cost/benefit analyses of different actions and values, the production of business cases justifying both privacy intrusions and the resulting implications, and when public acceptability of the proposed project is analysed (Wright et al. 2011). Again, the focus is on the specific project to hand. There is the possibility here to take a more collective view within such assessments; however, for our purposes this would require knowledge of the current state of SOSTs operating within a society so as to form a clear picture of the status quo. It is doubtful those undertaking the PIA would have access to such information or the resources to acquire it. Recently the concept of Surveillance Impact Assessment (SIA) has been developed, described as a ‘methodology for identifying, assessing and resolving risks, in consultation with stakeholders, posed by the development of surveillance systems’ (Wright and Raab 2012: 613). The SIA concept seeks to increase stakeholder engagement, minimise the impact of surveillance technologies, and improve upstream development. However, this initial conceptualisation still appears to focus on the individual technology and not the collective assessment of other existing SOSTs within its methodology. Whether this changes in practice remains to be seen.

Finally there are public consultations on SOSTs, an example being the consultation on the operation of airport whole body scanners within the UK. Often balancing is integrated into these documents through the framing of the issue for discussion. For example, in relation to body scanners the government’s position was that:

> [u]ltimately the rights of individuals must be balanced against the need to protect passengers and others at risk from terrorist threats and accordingly the use of security scanners in accordance with the interim code of practice is, we believe, proportionate in these circumstances.

(DfT 2010: 9)

However, by restricting the questions to body scanners alone, and not the combined effect of all aviation security measures, again the focus of this consultation is directed inwards.

None of these comments are intended to criticise these methodologies in any way. They all perform valuable functions in assessing individual technologies. Rather this discussion seeks to highlight both the prevalence of balancing within assessment methods and their predominant focus on individual technologies as opposed to a more comprehensive stance.

---

12 Department for Transport (DfT) Code of practice for the acceptable use of advanced imaging technology (body scanners) in an aviation security environment. A consultation paper.
5. How the individual assessment of SOSTs eventually abolishes privacy

As stated in the introduction, I posit that when assessing new SOSTs which impact upon privacy, we need to do so by examining the combined effect of all such security technologies currently employed within the society we are examining. Failing to adopt this collective approach will inevitably lead to a society where surveillance is absolute and privacy is extinguished. This argument is informed by the preceding discussions on the nature of privacy and security, the act of balancing, the pressure to produce new SOSTs, and the current individually-focused assessment methodologies. By drawing together the various elements of these discussions I justify my conclusions using the following arguments:

Two assumptions underlie my position. The first is that the assessment of whether individual SOSTs are appropriate for deployment often entails a judgement of whether any loss in privacy is legitimised by a justifiable increase in security; representing the ubiquitous balancing metaphor. As discussed in detail earlier, the concept of balancing is unavoidable as it pervades our political and legal systems. It is also invaluable in that it forces decision makers to acknowledge the presence and weight of rights concomitant to security, and opens up their decision making processes to a measure of scrutiny. However, balancing is also beset with flaws; it is arbitrary and subjective, lacking in meta-rules, and purports to successfully compare objects (such as privacy and security) which possess different intrinsic characteristics.

Focusing and expanding upon this final point, one of the fundamental differences between privacy and security is that only one of them has two attainable end-states. Privacy \((P)\) exists as a finite resource on a quantifiable spectrum with two attainable end-states; that being absolute privacy \((P=1)\) at one end through to the absolute absence of privacy \((P=0)\) at the other. Whereas security \((S)\) also exists as a finite resource but on a quantifiable spectrum with only one attainable end-state; that being the absolute absence of security \((S=0)\). However, as discussed earlier, absolute security \((S=1)\) can never be achieved and therefore must exist as a desirable yet ultimately unobtainable goal always equating to something less than 100 per cent \((S=<1)\); hence the absence of a second attainable end-state.

The second assertion, which follows from and builds upon the first, holds that one consequence of absolute security being unobtainable yet desirable is that new SOSTs will continuously be developed in a futile search for this unobtainable goal. These technologies each potentially trade a small measure of privacy for a small rise in security. This production process is driven by a variety of internal and external sources beyond the conflicting internal characteristics of security and privacy. These include; the nature of fear and risk, pressure by politicians and police, the availability of funding, push by the security industry, and public support for these technologies. These factors operate together to ensure a fertile environment exists for the research and development processes of the security industry to thrive.

To be afforded legitimacy, ensure legal compliance, and to minimise negative social responses, each new technology needs to be assessed before deployment. Predominantly this entails use of the balancing metaphor. Current assessment methodologies focus on the benefits and impacts of the individual technology that is being proposed. When examined individually, each of these surveillance technologies may legitimately justify any related privacy/security trade-offs. Assuming the validity of the first assertion regarding the different natures of security and privacy, this second assertion holds that as more and more individually assessed SOSTs are introduced to operate simultaneously within an environment in the quest for ever greater security, privacy will ultimately be reduced to zero.

This is one of the unforeseen consequences of balancing security against privacy when privacy is finite and absolute security is unobtainable. A potentially infinite number of SOSTs can be developed, each producing a measure of additional security while entailing the sacrifice of a commensurate measure of privacy. Yet as absolute security will never be obtained, the motivation to produce ever more technologies...
will remain. Meanwhile at some point the cumulative sacrificing of privacy will reduce its quantum to zero despite the still present security risk.

If one both accepts the argument as set out above as true and holds privacy to be a right worth preserving, then it becomes clear there exists the need to supplement, as opposed to replace, the current focus on individual technology assessment with a system of collective assessment. Thus the privacy reducing implications of all SOSTs currently operating within a society would be taken into account when assessing whether or not a new security measure can be justified. If a society fails to adopt this collective approach there will be no effective holistic mechanism for preventing the inevitable slow march into a total surveillance society.

6. Complementing individual with collective assessment

By collective assessment I refer to a process whereby the acceptability of a new SOST is determined by assessing its effects in combination with other SOSTs already operational to determine both the necessity of this new entrant and the resultant quantum of proportionality\(^{13}\) if the new technology was adopted. This collective approach is not intended as a replacement for existing assessment methodologies which determine the acceptability of each individual technology, rather it would complement them by forming a secondary assessment step. Hence if the technology is individually unacceptable it would be rejected outright without the need for collective assessment.

Any adoption of a collective assessment methodology for the purpose of retaining privacy would be premised on a number of requirements. Firstly it requires citizens (or at least the majority) not wanting to actually live in a surveillance society where their physical, communication, location, and personal data is routinely collected and/or processed so as to maximise their individual and collective security. This position entails the concomitant acceptance of insecurity as the natural condition; i.e. the conscious understanding and acceptance that absolute security can never be achieved regardless of how many security measures are introduced. This also needs to be coupled with an appreciation of the value of other rights and freedoms (besides security) to temper the temptation to introduce ever more SOSTs. I must stress here that this desire by citizens to oppose a total surveillance society is by no means given. Privacy and security are social constructs; the different weights assigned to them exist differently across societies, are contextual, and change over time (Solove 2009: Ch.3). It is completely conceivable that a given society at a given time and/or under given circumstances, may desire to live in a surveillance society. At this point they may still wish to adopt a collective assessment methodology for the purpose of identifying areas of social existence requiring additional surveillance as opposed to the purpose of preserving privacy.

Secondly, collective assessment requires a general acceptance that privacy has to be retained; that once privacy levels are reduced to a certain level, any further reductions cannot be justified regardless of the competing right. If this consensus does not exist (regardless of where these levels are set) then the total surveillance society envisioned within my paper will occur. If there is nothing within the act of living within a society that most/many citizens believe should remain off limits to surveillance, then this view represents tacit approval for a total surveillance society; if nothing is off-limits then everything becomes a valid target.

On the assumption however that a society wishes to preserve a certain level of privacy, this could conceivably be achieved through different methods and protections. I have set out three below which could operate either individually or in combination.

---

\(^{13}\) Being the proportionality of all operating SOSTs, including the proposed technology being assessed, given the security they afford and the resultant infringement of privacy.
The first option is to designate certain objects as *prima facie* ‘off-limits’ to surveillance. This could include; certain geographical locations (individual homes, wider community spaces, streets, work-spaces, etc.), certain data (geographical, communication, internet, etc.), and/or certain physical actions (correspondence, physical interactions, etc.). In the event of reasonable suspicion that an individual is committing offences within one of these restricted areas a surveillance warrant could be issued by a judge.

The second option is to ban certain actions by law enforcement agencies. This might include:

- any form of stop-and-search without reasonable suspicion (and suspicion could not be inferred simply because somebody is physically present within a certain geographical location\(^\text{14}\));
- any form of data-mining where it either equates to a fishing expedition or where if the data being sifted was not digitally available a warrant would be required to gain access to it;
- and prosecutions based on targeted surveillance where no prior reasonable suspicion existed justifying that surveillance.

A third option is to use citizen juries in conjunction with political and/or judicial bodies to monitor and limit the current surveillance options available to law enforcement agencies within a society. They would be afforded complete oversight such that only SOSTs and measures approved by these bodies would be lawful. No surveillance, or prosecution based on surveillance, outside of these designated limits would be permissible.

There are challenges with all these options, with each raising difficult questions. On the idea of setting surveillance limits, who would decide where these limits are set and how would they go about doing this? How easy would it be to modify these limits, and under what circumstances would this occur? On the option of fettering the activities of law enforcement agencies, how would this be policed and what would happen if officers discovered information pertaining to a crime whilst themselves engaging in illegal surveillance activities? And on the option of citizen juries, how would these be empanelled, who could sit on them, and what oversight would exist?

The presence of such challenges does not automatically negate the viability of any of these options. This is merely an acknowledgement that any method adopted should be done so with caution and considerable foresight. That said, the ideas set out above are achievable for they reflect values and norms that are currently observable within UK society. Despite the preoccupation with security leading to the spread of SOSTs throughout society, both UK citizens and their government still protect certain areas from interference and consider certain actions unacceptable. The home and bedroom are still somewhat protected from intrusion in that police are not (yet) allowed to randomly enter homes to search for evidence of crimes without prior suspicion or evidence of an offence. Written and oral communication between suspects or prisoners with their legal representatives is still largely protected, and the use of torture is thankfully still considered beyond the pale for the majority of citizens. And yet all of these actions have the potential to uncover evidence of criminal offences.

These examples show UK citizens are not yet willing to sacrifice every concomitant right on the altar of security, and while this holds true the opportunity remains to introduce measures for protecting privacy and scaling back the surveillance society. Collective assessment is a step down this path in that it makes explicit the current overall balance between security and privacy, thereby raising citizen awareness of the state of their society. Nevertheless, if privacy is valued at least as much as security is valued then this collective assessment needs to be backed up with protection measures such as those outlined above. Without these measures any such assessment is merely an exercise in collecting and collating information. It will tell us how far away we are from the oncoming train that is the absolute surveillance society.

\(^{14}\) Thus requiring a repeal of Section 44 Terrorism Act 2000.
without affording us the wherewithal to change its direction before we find ourselves forever wedged firmly under its wheels.

Acknowledgements
This research was funded by the Engineering and Physical Sciences Research Council of the United Kingdom through their Centres for Doctoral Training programme, specifically the Security Science Doctoral Research Training Centre (UCL SECReT) based at University College London.

References


