Unmanned Vehicles, Surveillance Saturation and Prisons of the Mind

COMMENT BY BRENDAN GOGARTY

Abstract

In this commentary I expand upon the discussion on privacy that I set out with my colleague in the précis to this edition. In particular I consider what the impact of military technologies, designed to achieve persistent and saturation capacity surveillance over war zones might be on civil space and civil society.

1 Introduction

Unmanned Vehicles (UVs) are lauded as 'force multipliers' but so too can they be seen as 'problem magnifiers', particularly for the law. That is, in very large part, because they are specifically designed to overcome traditional anthropocentric limitations, extending the reach and influence of their controllers into areas and arenas that the law previously needn't concern itself. In the précis we argued this was particularly apparent in respect of the increasing use of surveillance drones in the civilian space. The recent success of unmanned vehicles (UVs), particularly aerial UVs (UAVs), is very much the result of their capacity to undertake 'high-powered and constant surveillance over vast tracts of land' in conflict zones.[1] Given the majority of current civilian UV technology — especially those employed by state entities — is merely rebadged military adaptations, we argued that their 'adoption into the civilian world will provide the same surveillance capacities to those controlling them; capacities far beyond those envisioned by the Courts of both those countries that recognise a right to privacy, and those that do not'.[2] In this commentary I wish to examine the socio-legal implications of so-called 'global, persistent, surveillance'[3] by UVs employed by the state, over its own, rather than enemy territory. In particular, I will consider the potential impact on privacy and how the erosion of personal privacy will ultimately impact on other freedoms important to civil democratic societies, such as freedom of expression and freedom of association.

This commentary will start with a basic overview of privacy and surveillance. Following this I will discuss how surveillance may impact on certain important privacy rights and consider how UV technologies threaten to erode

1 Brendan Gogarty and Meredith Hagger, 'The Laws of Man over Vehicles Unmanned: The Legal Response to Robotic Revolution on Sea, Land and Air' (2008) 19(1) *Journal of Law, Information and Science* 73, 130 ('précis').

2 Ibid 130.

3 Ibid 80.

those rights much further. I contend that current law is insufficient to act as a check on the over use or misuse of UV surveillance and argue that some form of regulatory debate is required to address current regulatory shortcomings.

This commentary is not intended to recommend or frame possible regulatory responses to that attrition of civil rights. Rather I argue that, should the requisite public and legal debate not happen soon, then it will not only be relatively futile, but that, ironically, it may impact on people's willingness to participate in democratic and participatory activities in the first place.

2 *Privacy and Surveillance: Definitions*

Before examining the impact of UVs on privacy it is important to discuss what privacy is. Unfortunately this is not a particularly easy task. Indeed, it is almost impossible to write about privacy without noting its definitional, conceptual and legal problems.

2.1 Privacy

Privacy is 'somewhat of an esoteric concept, without precise objectively discernable boundaries'.[4] It covers a wide range and forms of behaviour, can be context dependent and subjectively variable.[5] The term can describe everything from interpersonal infringement of body space, to eavesdropping, computer hacking or surveillance by the state. In the précis we covered a larger range of these sub-categories[6] than I plan to discuss here.

What I intend to focus on is the notion of privacy as a 'right to be left alone',[7] particularly from interference and monitoring by the state and its institutions. Specifically I wish to consider the far-reaching consequences of the temporal and physical extension of state surveillance that UV technology now makes possible. I believe this is the most worrisome immediate problem presented by civilian UV technology, at least in the near future.

2.2 Surveillance

Unlike the more nebulous concept of privacy, surveillance is somewhat more of a defined construct. Surveillance, according to James Rule, entails 'any form of systematic attention to whether rules are obeyed, to who obeys and who does not, and to how those who deviate can be located and sanctioned.'[8] Anthony Giddens described surveillance as the 'the supervision of the

4 Précis, above n 1, 126.

5 Daniel J Solove, 'Conceptualizing Privacy' (2002) 90 *California Law Review* 1087, 1092.

6 Précis, above n 1, 124-132.

7 Samuel Warren and Louis D Brandeis, 'The Right to Privacy' (1890) 4(5) *Harvard Law Review* 193.

8 James Rule, *Private Lives and Public Surveillance* (Allen Lane, 1973) 40.

activities of subject populations', especially in the 'political sphere'.[9] He divides surveillance into direct (prisons/schools/workplaces) and indirect insofar as it relates to the authoritarian 'control of information' and the ordering and deployment of that knowledge.[10] Hence, in this paper the term is taken to mean the observation and recording of individuals' behaviour with the ultimate aim of ensuring rule compliance or metering sanction for rule breach.

2.3 Surveillance and privacy – the interface

Surveillance has seemingly direct and obvious implications for privacy, insofar as it results in the viewing and recording of individuals' behaviour and movement. It is often undertaken without the surveillance subject's consent and sometimes without their knowledge. Equally, once recorded, personal information may be re-used in ways, which the subject has not, or cannot be assumed to, have consented to. This would innately appear to be a fundamental breach of privacy. Yet, that innate sense does not always rationally translate into a clear form of actual harm. That is particularly the case where the surveillance is undertaken openly and in the public domain. Yet, sometimes it can even be hard to explain why covert surveillance causes harm or offense in the private domain, especially where the subject of the surveillance is unaware of it.

Much surveillance, particularly audio-visual surveillance, is undertaken in places where the subject would not or could not have a reasonable expectation of privacy.[11] In places like prisons, schools or workplaces direct surveillance occurs with either direct or implied knowledge or consent to being observed by the data subject. Equally, indirect surveillance of public places often does no more than observe and/or record what is open to the general public to view anyway. In a free and open civil society it is neither practical nor appropriate to limit who may watch another, or the manner by which they may do so.

Even if surveillance is surreptitious and not in a public place there may be, Posner points out, 'no rational basis' for a person to claim they are harmed by it.[12] There is clearly no physical harm done to a person if a photo is taken of them in their home, even if it is without their knowledge or consent. Moreover, Posner argues that if nothing is done with the photograph, and the person never finds out it was taken, then there is little cause to claim there

9 Anthony Giddens, *The Consequences of Modernity* (Stanford University Press, 1990) 59.

10 Ibid.

11 Inasmuch as that phrase relates to the concealment of information from others. See Richard A Posner, *Economic Analysis of Law* (Aspen Law & Business, 5th ed, 1998) 46.

12 Richard A Posner, 'Privacy, Surveillance, and Law' (2008) 75 *University of Chicago Law Review* 245.

was emotional harm from its creation.[13] Similarly, if a telephone is tapped, but only a computer system, listening for key words relating to criminal activity actually monitors it — assuming no such words are used during the conversation — then one might ask, what the harm is, or indeed if anyone's privacy is *actually* breached.[14] To adopt Posner's reasoning, if you are not an antisocial or dangerous person, then there is 'no rational basis' to claim harm from being surveilled, when all that is being monitored for is dangerous antisocial behaviour.

Proponents of state surveillance often defend that position on the grounds that no harm is done, unless those being observed are doing something wrong to begin with. In other words, 'if you've nothing to hide then you've nothing to fear.' Of course the problem with that position is that it treats all of those being watched as potential rule breakers, whether they are or not. Assuming the surveillance is unidirectional it places the watchers in a position of perpetual oversight and power over those under their gaze, whether those people ostensibly should have had a reason to fear in the first place. Finally, it amplifies the power of the watchers to determine what should be feared. Privacy and surveillance scholars such as Goold therefore argue that, 'we should resist the spread of surveillance not because we have something to hide, but because it is indicative of an expansion of state power'.[15] It is perhaps in this sense — that is, the use and abuse of surveillance information by the state — that a compelling case can be made against unfettered and unconstrained surveillance as an abuse of the right to privacy.

2.4 Surveillance as an extension of state power

Whilst some civil libertarians deride any surveillance as a breach of a fundamental right to be 'left alone',[16] the reality is that there has never really been an absolute right in any society for citizens to keep all information about themselves secret and away from the prying eyes of others.[17] Indeed, the idea

---

13 Ibid.

14 Indeed, one might argue, there is actually little difference if it was a human rather than computer listening in to that conversation, inasmuch as that human would be better trained to discount innocuous references to, say terrorism, and allow the remainder of the conversation to go unrecorded.

15 Benjamin Goold, 'How Much Surveillance is Too Much? Some Thoughts on Surveillance, Democracy, and the Political Value of Privacy' in D W Schartum (ed) *Overvaaking i en Rettstat (Surveillance in a Constitutional Government)* (Fagbokforlaget, 2010) <http://ssrn.com/abstract=1876069>, 44.

16 For a good overview of the normative status of privacy as a right see, Waldo et al, *Engaging Privacy and Information Technology in a Digital Age* (National Academies Press, 2001) 66-69.

17 Indeed privacy as a legal concept only really arose in the nineteenth century, and then as a standalone 'right' in some countries, but not others. That said, the right has become more doctrinally accepted at an international, and multinational level. Indeed in Britain and most other common law countries, courts have been rather inimical to an enforceable common law right to privacy, even against the state, in

of privacy as a right, particularly a human right, is a relatively recent legal concept and one which is intertwined with the development of surveillance technologies.

One of the major, if not the primary, catalysts for the development of domestic and international privacy law has been as a response to monitoring and recording technologies. The invention of the instamatic camera drove the development of the US tort of privacy.[18] Later developments in privacy law at the international level can similarly be seen to be a reaction to the adoption of increasingly powerful and invasive surveillance technologies during the cold war, when spying on foreigners and one's own citizen's became a central apparatus of state intelligence and defense.[19] More recently, transnational data protection laws have been developed as a consequence of the introduction of international telecommunications networks, the Internet and now portable digital communications.[20]

The exception to this general trend has been open public surveillance, particularly of the audio-visual variety. Public surveillance has not received a great deal of regulatory attention or intervention, despite the rapid and near exponential growth of closed-circuit television (CCTV) — especially by state organs — in public spaces over the last four decades.[21] The preponderance of this public surveillance technology, particularly by state institutions, and the seeming complacency about it amongst a large proportion of the public has worried scholars and civil libertarians concerned about its potential impact on civil rights.[22]

2.5 Surveillance and civil rights

The potential impacts of surveillance on civil rights have been subject to analysis, discussion and debate by scholars, philosophers and lawyers for a significant period. Perhaps the most seminal early work was that Jeremy Bentham in 1787 as part of his *Panopticon Letters*,[23] a treatise on the design of

---

the absence of legislative protection. That position is different in other jurisdictions which recognise a right to privacy, and in international and multilateral agreements such as the ICCP and ECHR. See Dorothy J Glancy, 'The Invention of the Right to Privacy' (1979) 21(1) *Arizona Law Review* 1.

18 See n 63. See also, Robert E Mensel '"Kodakers Lying in Wait": Amateur Photography and the Right of Privacy in New York, 1885-1915' (1991) 43(1) *American Quarterly* 24.

19 See generally, Deborah Nelson, *Pursuing Privacy in Cold War America* (Columbia University Press, 2002).

20 Michael Kirby, 'The History, Achievement and Future of the 1980 OECD Guidelines on Privacy' (2010) 20(2) *Journal of Law, Information & Science* 1.

21 Caoilfhionn Gallagher, 'CCTV and Human Rights: the Fish and the Bicycle?' (2004) 2(2/3) *Surveillance & Society* 270.

22 Ibid.

23 Jeremy Bentham, *The Panopticon Writings* (Verso, 1995) e-version available from <http://cartome.org/panopticon2.htm>.

an efficient prison system. That system was designed around the (then) nominal idea that prisoners would be placed in cells where they always might be observed by prison officers, but could never actually know if they actually were; the prison cells were permanently lit whilst officers were to be placed in an obscured and darkened guard tower. Bentham argued this system would be effective because,

> the more constantly the persons to be inspected are under the eyes of the persons who should inspect them, the more perfectly will the purpose [of social/behavioural control] … have been attained. Ideal perfection, if that were the object, would require that each person should actually be in that predicament, during every instant of time. This being impossible, the next thing to be wished for is, that, at every instant, seeing reason to believe as much, and not being able to satisfy himself to the contrary, he should *conceive* himself to be so.[24]

In other words, people will generally modify their behaviour to comply with rules when they are being watched by those with the power to sanction or punish rule breaking. However, they are also likely to modify their behaviour if there is a *possibility* of being watched by those authorities. That is, the uncertainty of whether someone is being observed can create the same effect on someone as actually observing him or her.

Bentham's system greatly increases the administrative efficiency of monitoring and controlling subject populations, by reducing the locus of that control from a one-to-one ratio to a one-to-many ratio. It achieves this power differential by placing a larger cohort on notice that they *may* be being observed by one or more watchers at any one time, whilst simultaneously denying them the capacity to confirm they *actually* are.[25] Foucault, who built his work upon Bentham's — and who is equally a standard reference in most surveillance literature — described the uncertainty control principle of surveillance as a 'diagram of a mechanism of power reduced to its ideal form… it is in fact a figure of political technology that may and must be detached from any specific use'.[26]

3 Towards a 'Surveillance Society'

Bentham's ideas were both lauded and criticised, but gained little practical traction in practice, either in respect of prison populations or social and population control more generally. That was until the advent of modern audio-visual recording technology which allowed for the installation of recording devices to allow for efficient monitoring of both public and private

24 Ibid.

25 Indeed it is possible that, sometimes at least, no one may actually be watching at any one time; but as long as the subject population does not know that, the effect should be the same.

26 Michel Foucault, *Discipline and Punish: The Birth of the Prison* (Patheon, 1977) 205.

spaces. CCTV cameras in particular have resulted in vast areas of public and private space being monitored and surveilled by a range of entities, but particularly state ones.[27] Added to this is the fact that much human interaction now occurs via technological means and conduits, from telephones to the internet, all of which may be monitored and surveilled, with or without the participants' knowledge. This turned many western countries into what some scholars describe as a 'surveillance society' given that so much of people's lives in these countries is actively monitored, or at least capable of being monitored.[28]

Given the rise of the so-called surveillance society, it might be expected that the early theories of Bentham and others would finally be proven or disproven. Ultimately however, there is a lack of solid evidence that panoptic surveillance is an effective or ineffective mechanism to ensure social control.[29] On the one hand, studies of small groups show that the panoptic effect of uncertainty does result in self-regulation in controlled situations.[30] Panoptic designs have also been integrated into workplaces, and some studies indicate they are successful in increasing productivity, safety and efficiency, especially where the work is in a controlled environment or centres upon electronic communications (for instance, call centres).[31] Other studies are less conclusive or argue that the negative affects of the constant monitoring undermine rather than promote worker morale and satisfaction and thereby reduce efficiency.[32] Outside of controlled studies of small groups the evidence is even more controversial. For instance, some statistics seem to indicate that the introduction of CCTV cameras may reduce crime and anti-social behaviour,

27 Gallagher, above n 21, 23.

28 David Lyon, *The Electronic Eye: The Rise of Surveillance Society* (University of Minnesota Press, 1994) 57-80.

29 As Vorvoreanu and Baton note, 'The paradox of electronic surveillance is that it is much used and little understood.' Mihaela Vorvoreanu and Carl H Botan, 'Examining Electronic Surveillance in the Workplace: A Review of Theoretical Perspectives and Research Findings' (paper presented at Conference of the International Communication Association, Acapulco, June 2000) 3.

30 For instance, students will avoid prohibited websites when they know their Internet browsing history may be reviewed. S Dawson, 'The impact of institutional surveillance technologies on student behavior" (2006) 4(1/2) *Surveillance and Society* 69; see also Stuart Moran, Isaac Wiafe and Keiichi Nakata, 'Ubiquitous Monitoring and User Perceptions as a Persuasive Strategy' (2011) 3 *Web Intelligence and Intelligent Agent Technology* 41, doi: 10.1109/WI-IAT.2011.112.

31 Shoshana Zuboff, *In the Age of the Smart Machine* (Basic Books, 1988) 322; Jengchung Chen and William Ross, 'Individual differences and electronic monitoring at work' (2007) 10(4) *Information, Communication & Society* 488 doi: 10.1080/13691180701560002.

32 John R Aiello and Carol M Svec, 'Computer Monitoring of Work Performance: Extending the Social Facilitation Framework to Electronic Presence' (1993) 23(7) *Journal of Applied Social Psychology* 537, doi: 10.1111/j.1559-1816.1993.tb01102.x; Marylène Gagné and Devasheesh Bhave, 'Autonomy in the Workplace' (2011) 1(2) *Human Autonomy in Cross-Cultural Context* 163, doi: 10.1007/978-90-481-9667-8_8.

whilst other statistics seem to indicate the opposite, or merely show that the locus, nature and form of the activity shifts without reducing its quantum *per se*.[33] Indeed, some of the critics who argue that CCTV limits fundamental freedoms simultaneously cite its lack of impact on crime as a reason for its abolition.

Perhaps the most that can be said is that, ultimately, it is impossible to truly measure the impact of open surveillance on the population as a whole. Nevertheless, there is evidence that at least some people will be concerned about the monitoring, and, on a small scale at least, will self-regulate. Whilst those involved in crime might find ways around the surveillance,[34] or become nonchalant about it, those who are not involved in or intending to commit crime are still affected by it. In other words, surveillance treats all citizens as potential criminals and puts all on notice they are being watched for possible non-compliance with state authority.

One of the main attacks on unfettered state surveillance is that it may have a panoptic affect on those who challenge or dissent against state authority, but probably more importantly those who might wish to hear, interact or agree with them.[35] Governments have an interest in self-preservation, particularly from those who might undermine their authority, even in civil, democratic societies. Democracy however, can only flourish in an environment in which people are free to say and think what they wish, without fear of retribution or sanction for disagreeing with state policy or practice.[36] Democracy can also only flourish where people are free and unafraid to listen to such ideas and judge the veracity of them for themselves. As Emerson writes, '[a]n individual is capable of [democratic participation] only if he can at some points separate himself from the pressure and conformities of collective life.'[37] If there is nowhere for citizens to have such interactions without being fearful of the

---

33 A good meta-analysis of the competing statistics is provided by Brandon Welsh, and David Farrington, 'Public Area CCTV and Crime Prevention: An Updated Systematic Review and Meta-Analysis' (2009) 26(4) *Justice Quarterly* 716 doi: 10.1080/07418820802506206; see also William Webster, 'CCTV policy in the UK: reconsidering the evidence base' (2007) 6(1) *Surveillance & Society* 10; Sam Waples, Martin Gill and Peter Fisher, 'Does CCTV displace crime?' (2009) 9 *Criminology and Criminal Justice* 207, doi: 10.1177/1748895809102554.

34 Simon argues about open surveillance, 'the post 9/11 security situation is that the individuals one hopes to detect are the very individuals that have the best chance of evading detection.' Bart Simon, 'The Return of Panopticism: Supervision, Subjection and the New Surveillance' (2005) 3(1) *Surveillance & Society* 9.

35 Such views are not new, US Justice Felix Frankfurter stated in *Wolf v Colorado*, 338 U.S. 25 (1949) that, the 'security of one's privacy against intrusion by the …[state]– is basic to a free society'.

36 As Keith Boone puts it, privacy is 'vital to a democratic society [because] it underwrites the freedom to vote, to hold political discussions, and to associate freely away from the glare of the public eye and without fear of reprisal.' See C K Boone, 'Privacy and Community' (1983) 9(1) *Social Theory and Practice* 8.

37 Thomas I Emerson, *The System of Freedom of Expression* (Random House, 1970) 546.

gaze of the state, then there is likely to be an impact on the exchange of political ideas. Hence, surveillance scholars like Goold argue that:

> one of the greatest dangers of unfettered mass surveillance is the potential chilling effect on political discourse, and on the ability of groups to express their views through protest and other forms of peaceful civil action … [making it] harder for dissent to flourish or for democracy to remain healthy and robust …[and] the individual is always at the mercy of the state, forced to explain why the government should not know something rather than being in the position to demand why questions are being asked in the first place.[38]

Solove goes further and argues that,

> Surveillance is a different kind of privacy problem than disclosure, imposing a different type of injury to a different set of practices. Surveillance differs from disclosure because it can impinge upon practices without revealing any secrets. Being watched can destroy a person's peace of mind, increase her self consciousness and uneasiness to a debilitating degree, and can inhibit her daily activities.[39]

One must, of course, be cautious about overstating the impact of surveillance on political discourse, just as one must be cautious about overstating its impact on crime. Nevertheless, there is at least some evidence to suggest the panopticon effect operates to deter people from engaging in behaviour that might result in sanction. As major or minor as that impact might be, it is an impact all the same; an impact which will mean that we cannot ever describe our speech or association as completely free. The question is just how much of an impact we are willing to accept, and, once the boundary line is drawn, how we will limit further incursions and encroachment.

UV technology may just be the tipping point beyond which we can safely say there will be a real 'chilling effect' on political discourse, insofar as such technology promises to greatly increase the surveillance capacity of state organs. Surveillance capacity, according to James Rule is determined by examining the:

1. size and scope of files in relation to the subjected population;
2. centralization of those files;
3. speed of information flow; and
4. number of points of contact between the system and its subject population.[40]

---

38 Goold, above n 15, 43.

39 Solove, above n 5, 1130.

40 Rule, above n 8, 38.

As was discussed in the précis to this edition, UV technology dramatically increases the 'degree and scale' of all of these things:

> [The] concern about drones is how they may facilitate increasingly broad ranging, invasive and covert monitoring by the state, and possibly private companies and individuals … Unlike current surveillance systems, which tend to involve fixed, visible camera systems in public spaces, UVs will provide highly mobile and generally undetectable surveillance of any area within the relevant jurisdiction. Current UV applications could easily permit a person to be watched as they travel from home to work without their knowledge. Without some constraint, it is possible that covert surveillance will be ubiquitous in the not too distant future.[41]

UVs, particularly UAVs, permit an almost infinite number of points of contact with the population, because of the large and unmarked zones which they may surveil. Indeed, the fact that they are designed to operate without detection and from roving locations increases their panoptic effect, because, unlike modern CCTV cameras, a person can never know if a camera is actually watching them. Furthermore, much contemporary UV technology has been developed for intelligence, surveillance and reconnaissance (ISR) missions in war zones, specifically to collect vast amounts of audio-visual data over massive geographic areas. This generates massive amounts of ISR data that requires complex hardware and software systems to process and refine.[42] ISR data can be stored on conventional data systems at a later stage to review suspect sites and persons at a later date.[43] It is stored in highly centralised and interconnected within state data servers. When considered against Rule's criterion, this is a level of surveillance capacity nearly reaching saturation point.

3.1 Towards surveillance saturation

Although states are currently capable of employing UVs in a manner through which they might potentially achieve surveillance saturation, that is not yet, entirely a reality; but in the absence of immediate law and debate, it is a fast approaching possibility. Already we are seeing a push by state agencies to adopt UV technology as an efficient and convenient solution to civilian policing and security.[44] Indeed, the civilian transition of the technology is almost as rapid and exponential as its uptake in the military sphere post 9/11.

---

41 Précis, above n 1, 126.

42 Eli Lake, 'Drone footage overwhelms analysts', *The Washington Times* (online), 9 November 2010 < http://www.washingtontimes.com/news/2010/nov/9/drone-footage-overwhelming-analysts >.

43 In fact the ISR data collected by military UVs is so vast that it is practically impossible for human controllers to process it all. As noted in the précis, it is so wide ranging that nearly every part of Afghanistan may be under observation at any one time. Précis, above n 1, 137.

44 Ibid 106-108.

If that is the case, then UV technology will quickly become as ubiquitous — albeit in a less obvious or transparent way — as that earlier surveillance technology, such as CCTV. That means, without proper debate, we may very well experience the same privacy creep in the use of UV technology that we saw previously with CCTV.

The real effect of the move towards persistent, saturation level surveillance of civilian areas is, of course, also speculative. Nevertheless, there is good cause to assume it will have some affect on people's feeling of freedom to associate and participate in democratic forms of activities which may be unfavourable to, or sanctioned by, the government of the day. For instance police have increasingly turned to videoing protesters with handheld cameras, even at peaceful demonstrations.[45] The response by protesters has been to obscure their faces to avoid identification; and therefore they can, absent of being arrested, assume their privacy is maintained after they quit the protest. The difference in a world of UV surveillance is that those protesters cannot expect to return to anonymity once they leave the protest march and return to their homes and lives. Instead there is a very real chance they may be singled out and followed, silently and unknowingly from the scene of the protest all the way to their home. This is not a dystopian prediction, but rather a very real-world scenario exemplified by the killing of Tariq Azizm in Pakistan in late 2011, which is discussed in the commentary by Hagger and McCormack in this edition.[46]

3.2 Tariq's legacy

Tariq Azizm was killed after attending a meeting, called a 'Waziristan Grand Jirga' — best explained as a hybrid parliament/courtroom — in Islamabad, Pakistan.[47] He had been invited to attend that meeting, along a large group of villages from rural Pakistan, to commemorate drone strike victims and discuss the ongoing impact of such strikes on their own lives with western journalists.[48] Pakistan prevents journalists from entering tribal areas to interview or document drone strikes themselves.

At the Grand Jirga village elders refuted US Government claims that drone strikes were targeted, discrete and did not result in civilian casualties. Because

45 Goold, above n 15, 39.

46 Meredith Hagger and Tim McCormack, 'Regulating the Use of Unmanned Combat Vehicles: Are General Principles of International Humanitarian Law Sufficient?' (2011) 20(2) *Journal of Law, Information & Science* EAP 23, 10.5778/JLIS.2011.21.McCormack.1.

47 Clive S Smith, 'For Our Allies, Death From Above', *The New York Times* (online) 3 November 2011 <http://www.nytimes.com/2011/11/04/opinion/in-pakistan-drones-kill-our-innocent-allies.html>.

48 Justin Randle, 'US Steps Outside the Law as the War on Terror Drones On', *Sydney Morning Herald* (online) 24 January 2012, <http://www.smh.com.au/opinion/politics/us-steps-outside-the-law-as-the-war-on-terror-drones-on-20120123-1qdsu.html>.

of the media blackout in that region, those claims could not be substantiated in a manner sufficient for journalists to publish them to the rest of the world.[49] Consequently, western journalists and charity workers present promised to provide training, equipment and support to volunteer villagers, to permit them to collect 'physical proof that civilians had been killed'.[50] According to reporters present at the meeting, only three people were actually willing to volunteer for such a role, given the serious risks such work entailed; Tariq Aziz was one of those volunteers.[51]

Approximately 72 hours after the meeting in Islamabad, Tariq and his 12-year-old cousin were killed as they drove their car to collect an aunt from a wedding in the rural city of Miran Shah in North Waziristan. It is alleged that two Hellfire missiles (ironically fired from a drone) struck the car, killing both occupants within a few hundred metres of their house.[52] The CIA, which is responsible for such operations, neither confirms nor denies such strikes, so the basis for such claims cannot be substantiated; nor can speculation about if, or how, Tariq was tracked from the Grand Jirga in the capital back to his home town in the provinces. One British human rights lawyer who attended the Grand Jirga claimed, 'a homing device may have been placed in Tariq's car, possibly as a "warning" to others not to raise objections to the drone killings.'[53] As Hagger and McCormack state, 'the accuracy of these reports is almost impossible to determine, as are the reasons why these boys were targeted; herein lies the source of controversy.'[54]

Regardless of whether the claims that Tariq Aziz was killed because of his participation at the Jirga are true, they have been accepted by much of the world's press, and, importantly, many of his tribespeople and countrymen. According to the journalists present at the Jirga, participants had already felt apprehensive about being identified as participants.[55] Indeed, the small number of volunteers to document drone strikes must also be taken as indicative of the fear those participants felt about the proposed data gathering

---

49 Pratap Chatterjee, 'Bureau reporter meets 16-year-old three days before US drone kills him', *The Bureau of Investigative Journalism* (online), 4 November 2011, <http://www.thebureauinvestigates.com/2011/11/04/bureau-reporter-meets-16-year-old-just-three-days-before-he-is-killed-by-a-us-drone/>.

50 Smith, above n 47.

51 Ibid. Tariq was said to be one of the few people with computer skills and was also excited about the possibility of being provided with, and trained to use, a digital camera. Pratap Chatterjee, 'The CIA's unaccountable drone war claims another casualty', *The Guardian* (online), 7 November 2011 <http://www.guardian.co.uk/commentisfree/cifamerica/2011/nov/07/cia-unaccountable-drone-war>.

52 Smith, above n 47.

53 Anon, 'Boys' killing belies US claim on drone strikes', *The Australian* (online), 7 November 2011 <http://www.theaustralian.com.au/news/world/boys-killing-belies-us-claim-on-drone-strikes/story-e6frg6so-1226187021609>.

54 Hagger and McCormack, above n 46, EAP 23.

55 Smith, above n 47.

activities. Yet those were entirely peaceful measures, designed to create awareness about, and transparency around, local and foreign government activities and claims. That would seem to be a contradiction of the values of democracy, popular involvement and accountability that western countries such as the US ostensibly stand for. Regardless of whether all the details of Tariq's story are true — indeed, perhaps the uncertainty and speculation about its veracity makes it all the more effective — it sends a compelling message of warning to those who might consider participating in such accountability activities in the future.

Whilst one might hope the consequences in the civilian sphere would be much less dire, Tariq's story indicates the potential consequences of a panoptic society in which there is near, if not complete surveillance saturation. Given the covert nature of much UV technology, a person living in a place where they are regularly employed as surveillance devices can never be sure when or where or why they are being watched. It is hard to imagine how such a situation would not create some reluctance amongst at least part of the population to participate in activities, or interact with people, that are unfavourable to the government of the day.

3.3 Finding a balance

As Goold argues 'we need [privacy] in order to live rich, fulfilling lives, lives where we can simultaneously play the role of friend, colleague, parent and citizen without having the boundaries between these different and often conflicting identities breached without our consent.'[56] Permitting states to increase their surveillance capacity to near saturation point threatens citizens' autonomy to balance and control such boundaries. That, of course, does not axiomatically mean we must prohibit states from employing such technology. Indeed, the horse has already bolted, so to speak, on restraining governments from undertaking mass surveillance. Moreover, there are real and genuine security, economic, social and public interest reasons for utilising public surveillance systems. UV technology will, no doubt, add to those benefits, by, for instance, making sure criminals cannot escape the law by undertaking criminal activity just outside of the sphere of an obviously placed CCTV camera.

Hence, we should not assume that it is only governments that will be attracted to the increased surveillance capacities provided by UV systems. The expansion in state surveillance capacity has not been received as critically or with as much widespread resistance as some may have originally predicted, so it cannot be expected that the additional reach provided by UVs will create a sudden public outcry. As McBride observes 'some people may welcome the introduction of additional technology that may catch or decrease criminal activity', whilst 'others are significantly more apprehensive about the

56 Benjamin Goold, 'Surveillance and the Political Value of Privacy' (2009) 1(4) *Amsterdam Law Forum* 4, <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1509393>.

widespread use of such technology'.[57] Ultimately we may need to find a balancing line between these competing interests.

4 The Limits of the Law

Justice Posner observes extra-judicially that:

> People hide from government, and government hides from the people, and people and government have both good and bad reasons for hiding from the other. Complete transparency paralyzes planning and action; complete opacity endangers both liberty and security.[58]

Ultimately the role of the law is to both regulate and provide a socially acceptable balance between these two important competing interests. Yet, as was argued in the précis paper, the common law at the very least is relatively ill equipped to deal with modern surveillance systems and the socio-political issues they present.[59] Without reiterating the entirety of that argument, the main reasons for this are:

- Many common law countries still do not recognise a tort of privacy.

  In countries without a tort of privacy, laws that traditionally protect privacy, such as nuisance, trespass or confidentiality have extremely limited applicability to any form of surveillance of a public space and little in the way of 'actionable rights against UVs that are used to survey their private property'.[60]

- In those countries (notably the US) that do recognise a tort of privacy — and to an extent where confidentiality is relied upon — it is based upon what a person might 'reasonably expect' to be safe from prying eyes. As technology becomes more accessible and ubiquitous, no person can reasonably expect not to be surveilled from one vantage point or another.

In his commentary, Jim Davis argues that some of these concerns are overstated, insofar as:

> the reasonable expectation of privacy arises not from the fact that the subject of the intrusion had no reason to suspect that he or she was being covertly watched, but from the fact that the conduct of the subject of the

---

57 P McBride, 'Beyond Orwell: The Application of Unmanned Aircraft Systems in Domestic Surveillance Operations' (2009) *Journal of Air Law and Commerce* 74, 629, 638.

58 Posner, above n 12, 246.

59 Précis, above n 1, 126-130.

60 Ibid 127.

> intrusion is such that a reasonable person would be highly offended if that conduct were published to the world at large.[61]

Davis therefore contends that 'that such an expectation of privacy is [not] becoming harder to maintain' even in the face of technological advances which increase the scope and degree of surveillance capacity by both private and state actors.[62] Davis' legal analysis in this respect is, of course, correct. However, courts have looked to a variety of factors to determine when someone may have a 'reasonable expectation' of privacy, or be 'highly offended' when their privacy is breached. In some instances the technological ubiquity of the device or measure utilised to surveil a person is relevant to establishing those objective standards, in other cases it is not. Furthermore, I would also argue that there is a very fine, if not largely artificial, line between having 'no reason to suspect' one is being watched and whether 'a reasonable person would be highly offended' at the watching and/or subsequent publication of data collected during it; particularly insofar as that distinction is used as a basis to contend that social expectations of privacy do not change as technology advances.

The highly offensive test is an objective one, ascertained by virtue of what a reasonable person might expect to keep private in the social and temporal conditions in which they find themselves. Such expectations *must naturally change* as society does and technology is a predominant motivator of anthropomorphic and structural change in society. Our movements, communications and interactions may be captured and recorded in ways that were simply unimaginable even a few decades before, let alone the centuries ago when much of our common law developed.[63] Two centuries ago a person

---

61 Jim Davis 'The (Common) Laws of Man Over (Civilian) Vehicles Unmanned' (2011) 21(2) *Journal of Law, Information & Science,* EAP 6, 10.5778/JLIS.2011.21.Davis.1.

62 Ibid.

63 It is important to remember that Warren and Brandeis' seminal article 'The Right to Privacy' which led to the adoption of a tort of privacy in the US, was largely written as a response to the invention of the instamatic camera two years before. The result of that invention by Kodak was no small degree of moral panic and outrage and the prohibition of cameras from tourist sites and beaches. That technology, Warren and Brandeis argued, 'invaded the sacred precincts of private and domestic life.' They referred, as support for that proposition, to an unreported case of Marion Manola, who in that same year brought an action in the New York Supreme Court for being 'photographed surreptitiously and without her consent.' That was notwithstanding the fact the photograph had been taken whilst she was performing on Broadway in public. Whilst photographing someone participating in a public spectacle could no longer be considered abnormal or offensive, the fact that Ms Manola was wearing stockings (tights) was enough for a court to consider the photograph sufficiently offensive to warrant an injunction preventing its sale or distribution and for Warren and Brandies to argue that 'the law must afford some remedy for the unauthorised circulation of portraits of private persons'. See Warren and Brandeis, above n 7; Robert E Mensel, '"Kodakers Lying in Wait": Amateur Photography and the Right of Privacy in New York, 1885-1915" (1991)

would have little reasonable expectation of having their image captured while transiting through a public place, and even less expectation of it being captured from above their house or property. Today digital technology is so ubiquitous that it is impossible to expect that one's image will not be captured wherever there is another person or whenever one is visible to the open sky.[64] Technology changes our sense of self and other's place in the world and how we interact with each other in it. It serves to modify our expectations, moral or otherwise and it changes what we are offended about, highly or otherwise.

There are, of course, times when the technological state of play is not particularly relevant to establishing an objective standard of what is reasonable or what is highly offensive; as I noted above, courts have taken into account a variety of considerations in this respect. In the précis we discussed the case of *United States v Knotts*,[65] in which the Court held that a tracking device installed in a car did not breach the occupant's privacy.[66] Key to that decision was the fact that a person travelling on a road could never reasonably expect not to be watched by others, or indeed monitored by authorities for legal compliance with road rules and the like. As such, the fact that an advanced technology had permitted a more efficient level of monitoring did not make the expectation of secrecy and privacy any more reasonable, or the fact that the occupant was being watched any more objectively offensive. Ultimately the relevance of the novelty or ubiquity of a technological surveillance system will turn on whether it dramatically alters the surveillance capacities of the surveillor in a manner which an ordinary person cannot be expected to have predicted or understood.

It is also true, that in some circumstances, common surveillance technologies, such as cameras with telescopic lenses, may capture information which an ordinary person may not have expected to be kept completely free from prying eyes, but which that person may have a reasonable expectation of privacy about nonetheless. As Davis notes, Campbell's case[67] was one of these situations.[68] However, the crux of the issue in *Campbell* was not the viewing so much as the disclosure *subsequent* to the viewing of a recognised category of confidential information — namely medical information about Campbell's rehabilitation — to third parties, who were not privy to the original viewing.

43(1) *American Quarterly* 24; Dorothy J Glancy, 'Privacy and the Other Miss M' (1990) 10 *Northern Illinois University Law Review* 401.

64 Hence, in US curtilage cases such as *Florida v Riley*, 488 US 445 (1989) and *Dow Chemical Co v United States*, 476 US 227 (1986) — which consider whether aerial surveillance of property breaches the right to privacy and the right against unlawful search — the court has been particularly concerned as to whether the surveillance equipment used was commonly available. Indeed, in the latter case the fact that the police used ordinary aviation and photographic equipment was in fact pivotal to the determination that the surveillance was legal.

65 460 US 276 (1983), 283.

66 Précis, above n 1, 129.

67 *Campbell v MGN* [2004] UKHL 22 ('*Campbell*').

68 Davis, above n 61, EAP 10.

That case has much less to do with surveillance as the transfer of data collated and recorded as a result of it. Indeed, as an equitable doctrine confidentiality law ordinarily only provides an injunction to restrain the use of the information collected, rather than punish or remedy for the damages caused in collecting it.

What these cases reveal, *in toto*, is that the common law can do very little to restrain state surveillance over public areas, and indeed private ones that are open to plain view from either the ground or on high. As most state surveillance data is not published to the world at large, there is little chance for people to argue their common law rights have been violated, because there is no evidence of harm, either to the person or their sensibilities. More to the point, the common law, particularly tort law, is remedial, not prospective; operating *ex-post-facto* to sanction past behaviour. It is not particularly adapted to limiting or controlling future behaviour in the absence of ascertainable or substantive proof of harm. Given that surveillance may occur without the knowledge of those watched, and in such situations, no person can claim to be more harmed than any other member of the community, such law is a poor mechanism to balance the competing social interests of privacy and security.

As I set out at the beginning of this commentary, the real harm, or at least the prevalent social harm arising from surveillance capacity saturation, is the fact that people simply don't know when, or if they are being watched, or for what purposes or how that information might affect them now or in their future lives. In the panoptic world it is the uncertainty about whether data is being collected which is most harmful, not the disclosure of that data to third parties *per se.* Moreover, the most overwhelming harm is to society as a whole — by undermining and eroding the fundamental institutions upon which it is based — rather than discrete individuals within it. Should we consider such harms detrimental to fundamental democratic values of freedom of thought, freedom of expression and freedom of association, then pre-emptive laws are required to limit the causative factor that reduces citizens' capacity or willingness to exercise these freedoms. In other words, it is proscriptive legislation, restraining state capacity to expand its surveillance capacities to, or close to saturation point which is required, not expanding or modifying civil law to remedy perceived harms once they occur.

4.1 Regulatory 'disarray'

As was noted previously however, despite long-standing academic debate and the derision of civil libertarians, the surveillance society has grown and expanded without a great deal of regulatory restraint. That is not to say no laws exist. Most countries do in fact have privacy and data protection laws, but their application to open, indirect surveillance is patchy at best. In the UK for instance, CCTV surveillance has generally been held to fall outside the *Data Protection Act*;[69] a rather strange oversight for the country in the world

[69] Simon Chesterman, *One Nation Under Surveillance* (Oxford University Press, 2011) 150.

with the highest concentration of this form of surveillance device. Indeed, although Europe more generally is considered to have the most comprehensive privacy and data protection laws in the world — by virtue of the European Court of Human Rights and the Directive on Data Protection Privacy — *Privacy International* reported at the conclusion of 2011 that:

> Surveillance harmonisation [in Europe] that was once threatened is now in disarray. Yet there are so many loopholes and exemptions that it is increasingly challenging to get a full understanding of the privacy situations in European countries.[70]

Certainly the massive uptake in surveillance technologies by all forms of bureaucratic and security agencies make it particularly hard to ascertain just how much or where surveillance is occurring. *Privacy International* argues that the 'cloak of "national security" enshrouds many practices, minimises authorisation safeguards and prevents oversight'.[71] In the security conscious United States, the situation is equally bad, if not worse. Chesterman points to 'the many actors in the intelligence community', not to mention domestic law enforcement and state agencies operating surveillance devices in the United States who 'may pose accountability difficulties through sheer complexity … [and] fragmentation of authority can pose practical problems in ensuring appropriate oversight.'[72]

Indeed, although accountability mechanisms do exist, including cross-institutional regulatory regimes to 'watch the watchers', the focus of legislative restraint on surveillance has, centred upon the collection of surveillance data, especially in the audio visual realm.[73] As Solove argues, the problem with this situation is that:

> Surveillance is a different kind of privacy problem than disclosure, imposing a different type of injury to a different set of practices. Surveillance differs from disclosure because it can impinge upon practices without revealing any secrets. Being watched can destroy a person's peace of mind, increase her self consciousness and uneasiness to a debilitating degree, and can inhibit her daily activities.[74]

There is certainly very little regulatory consideration of the collective impact of the *process* of mass surveillance — as opposed to individual surveillance for

---

70 Privacy International, *European Privacy and Human Rights (EPHR) 2010 Privacy International*, the Electronic Privacy Information Center (2011) 11 <https://www.privacyinternational.org/Ephr>.

71 Ibid.

72 Chesterman, above n 69, 212.

73 Ibid 151.

74 Solove, above n 5, 1130.

the process of criminal investigation.[75] That is, it overlooks the monitoring and tends to only be concerned with what is done with the recorded data or how it is disclosed. Like the civil law, privacy legislation tends to be more concerned with individual rather than social harm. Equally problematic is the fact that legislation tends not to operate at the macro level, nor evaluate the level of state surveillance capacity in a whole-of-government sense.

The reality is that existing privacy and accountability legislative regimes are not, as of yet, appropriate regulatory devices to tip the balance from an appropriate level to saturation level surveillance capacity (assuming that there is a line to be drawn). That is, not least, because they are not so much concerned with surveillance capacity as post surveillance data use. Whilst the latter issue is extremely important in respect of privacy, the former has serious and profound implications for civil and democratic rights.

5 Conclusion

As has been discussed at length in the précis and a number of other commentaries, UVs do not create new issues *per se*, so much as extend the influence, capacities and reach of their controllers and thereby expand and compound the social and legal problems relating to their intended use. In respect of surveillance, they greatly magnify the surveillance capacity of those controlling them, most worryingly state institutions.

There are, of course, a range of benefits promised by UV technologies, not least for policing, law enforcement and public safety. But it is important not to forget that this is a technology developed in the theatre of war. We must also remember that it is a technology that promises to realise a panoptic vision originally designed around maintaining control over prison populations; albeit now on a much grander society-wide scale. Of course, we already live in a surveillance society, but UVs are the technology which may close the remaining gaps in the open spaces where people could previously expect to be 'left alone'.

Unlike CCTV cameras UVs are, more often than not, designed to be covert and undetectable. Even if CCTV is now almost so prolific that it is hard to avoid it completely in a public place, UVs now render void the theoretical idea that state surveillance can be avoided in public. Moreover, because this technology is unmanned there will certainly be no *time* when one can hope not to fall under the gaze of unsleeping eyes.

The world of UV surveillance is absolute, global and persistent and it threatens to turn civilian spaces into the panoptic prison of Bentham's imagination, if not a physical prison, a prison of the mind. That is because, as Tariq's story shows us, people living in a surveilled world must be constantly

---

75 This distinction is evident in Australia in the form of the *Surveillance Devices Act 2004* (Cth), which limits the capacity of law enforcement agencies to undertake electronic surveillance of suspects or as part of investigations.

on their guard about whom they meet, what they talk about and whether those interactions might be with persons or about subject matters that draw the attention of a hostile state.

It is, of course, easy to overstate the impact of new technologies. Once the moral panic subsides, we have, as a society proven remarkably adept at subsuming technological advances into everyday life in a way that maximises their social utility and benefit. However, successfully integrating novel technologies in a manner which maximises their benefits and reduces their risks requires foresight, consideration and effective debate. Such debate and deliberation works most effectively in advance of technological change, and certainly in advance of the social change that it brings. That is a lesson from the nuclear proliferation debate, which is particularly relevant to UV technology and one highlighted in the précis paper.[76] Even since that paper was written the world has proceeded further into a UV arms race; most recently with Asia increasing its research and production in the area. Unchecked, there will be equally wide proliferation of the technology in the civilian sphere given the strength of support by proponents and governments for are its — as Mary Ellen O'Connell describes — 'seductive' qualities;[77] in this case: scope, efficiency, cost savings and reach.

The point of this commentary was not to suggest where the line should be drawn for the use of UV technology in civil society, nor the regulatory mechanism to achieve it. Rather it was to point out some of the socio-legal risks of unfettered proliferation of UV technology should we not take some form of action.

I have argued that the law does very little to restrain the use or impacts of UVs by state authorities. Ultimately, at present, the only real brake on reaching near saturation point state surveillance capacity is the speed of the transition from military to civilian spheres. As Chesterman rightly notes '[t]he notion that courts will have a leisurely opportunity to consider the implications of new surveillance technologies and their use now seems quaint.'[78] The same is true of legislatures and society as a whole. That means we are running out of time for debate and running out of time for effective regulatory responses should the debate determine some limits are required. Ironically, the unfettered and unrestrained use of surveillance threatens the very democratic institutions which operate to ensure that debate is effective and truly representative. That, more than anything else should be a motivating factor for real commitment to regulatory deliberation on the use of UVs in civil society.

---

76 Précis, above n 1, 142.

77 Mary Ellen O'Connell, 'Seductive Drones: Learning from a Decade of Lethal Operations' (2011) 21(1) *Journal of Law, Information & Science,* EAP 1, doi: 10.5778/JLIS.2011.21.OConnell.1.

78 Chesterman, above n 69, 154.