W Lamer 'From sleepwalking into surveillance societies to drifting into permanent securitisation: Mass surveillance, security and human rights in Europe' (2017) 1 *Global Campus Human Rights Journal* 393
http://dx.doi.org/10.25330/1465

From sleepwalking into surveillance societies to drifting into permanent securitisation: Mass surveillance, security and human rights in Europe

Wiebke Lamer*

Abstract: *The migration crisis, terroristic acts on EU soil and other so-called generators of risks have been accompanied by an increasing trend towards securitisation in many European countries. After decades during which traditional national security threats only indirectly affected most member states of the EU, many European governments have now turned towards policies that prioritise the safeguarding of national security at the expense of human rights and civil liberties. In countries that have been directly affected by Islamic terrorism, such as France and Belgium, extreme anti-terrorism legislation has been implemented and civil liberties have been curtailed. The threat of terrorism and the migration crisis has been accompanied by a legitimisation for the increased use of government surveillance measures for border control and counterterrorism actions. The article examines the linkages between securitisation and surveillance in the European context, and studies the consequences of the increasing trend of government surveillance on human rights. The article argues that looking at the implementation of mass surveillance measures in Europe illustrates that the continent is drifting into a permanent state of securitisation that threatens not only certain human rights, but the very foundation of democratic societies by permanently altering state-society relations. It also discusses possible ways to counter these worrying trends.*

Key words: *securitisation; mass surveillance; Europe; human rights; democracy*

1 Introduction

The migration crisis, terror attacks on European Union (EU) soil and other 'generators' of risk have been accompanied by an increasing trend towards securitisation in many European countries. The term 'securitisation' was coined by Buzan, Wæver and De Wilde in the 1990s. Securitisation occurs when an issue 'is presented as an existential threat, requiring emergency measures and justifying actions outside the normal bounds of political procedure' (Buzan et al 1998: 23-24). Processes to securitise the issues of migration and of terrorism in Europe are not novel,

* BA (De Montfort), MA (Leicester), MSc (London), PhD (Old Dominion University); EMA Teaching Fellow, EIUC; wiebke.lamer@eiuc.org. This article is based on a paper prepared for and presented at the Global Classroom, a project of the Global Campus of Human Rights, Bangkok, Thailand, 22-26 May 2017.

particularly since 9/11, and have been studied by securitisation scholars of various schools. However, following several terrorist attacks in Europe and the rise of populist parties across the continent who link the influx of refugees from the Middle East and North African (MENA) region with terrorism, many European governments have now turned towards policies that prioritise the safeguarding of national security at the expense of human rights and civil liberties.

France and Belgium, countries recently directly affected by Islamic terrorism, have implemented extreme anti-terrorism legislation that curtails civil liberties. Since the November 2015 terror attacks in Paris, France has been in a continued state of emergency. European countries that have not directly experienced any recent terrorist attacks also implement draconian counterterrorism laws (Amnesty International 2017). This is not least due to the fact that in many European countries, populist rhetoric has given rise to the notion that an increased number of refugees equals an increased number of terrorist attacks. The issue of migration thus is linked to the already securitised issue of terrorism, and both are further elevated above the merely political and into the existential threat territory, which legitimises breaking existing rules or implementing unlawful legislation.

Understandably, many observers in the human rights community have watched this trend unfold with concern. States of emergency in the wake of terrorist attacks become permanent; security becomes the go-to excuse for governments across the continent to curtail civil and political rights; and government surveillance powers become legitimised. In fact, surveillance is intrinsically linked to countering terrorism and, thus, highly relevant to the securitisation debate.

Surveillance is a tool used by governments. Surveillance is staged in securitising language. For example, in 2014 Theresa May, then UK Home Secretary, justified government steps to establish greater surveillance powers by stating that ensuring that police and security services have the right powers to uncover terror plots was now 'a question of life and death, a matter of national security' (Farmer 2014).

As the article shows, it may also be argued that surveillance tends to be moved outside the normal boundaries of political procedure. This is due to the fact that surveillance is framed as a necessary counterterrorism measure as in the example from the UK, and because much of it is conducted in secrecy; secrecy, one has to add, that is also justified in the name of national security.

Given these close links between surveillance, counterterrorism measures and national security, it is vital to take a closer look at surveillance in the context of securitisation. At this point it is worth noting that surveillance also comes with a host of other factors that further complicate its relationship with securitisation. For instance, surveillance itself has garnered considerable attention with regard to its potential to dangerously undermine human rights and democracy, particularly since the 2013 Snowden revelations. This, too, feeds into the processes of securitisation, which include governments using the justification of existential threats that require emergency action to break established rules. As the Snowden leaks showed, by using indiscriminate mass surveillance, governments were indeed breaking laws. What is more, the revelations

also showed that governments were not only using surveillance technologies for the purposes of countering terrorism. They also spied on allied politicians, journalists and human rights defenders.

Consequently, it is worth looking at the interplay between these issues in more detail, especially since we see evidence across the continent that security is becoming the dominating policy paradigm, enabling harmful practices such as mass surveillance, and creating an atmosphere in which security permanently becomes the foundation of political and daily life and discourse. Surveillance, of course, is a broad term and is not only carried out by governments. Surveillance by corporate entities is an equally disturbing phenomenon, and boundaries between surveillance by private and public actors are becoming increasingly blurred. This article, however, focuses on indiscriminate mass surveillance, including the collection and use of electronic (bulk or meta) data, by governments and their agencies.

The aim of the article is to examine the relationship between permanent securitisation, mass surveillance and human rights. The article contends that examining the implementation of mass surveillance measures in Europe reveals that the continent is drifting into a permanent state of securitisation that threatens not only certain human rights, but the very foundation of democratic societies by permanently altering state-society relations. Not only have we sleepwalked into surveillance societies in Europe, as UK Information Commissioner Richard Thomas first warned the UK in 2006, but we are also sleepwalking into permanent securitisation (Wright & Kreissl 2014: 320).

The article proceeds as follows: First, it outlines the current state of mass surveillance in Europe. It then turns to a discussion of the role of the public in the normalisation of mass surveillance, before outlining the impact of mass surveillance on human rights. Finally, the article examines the relationship between mass surveillance and permanent securitisation, and concludes with a discussion on how to counter these trends.

Throughout the article, four examples are highlighted in the context of mass surveillance and securitisation in Europe: France, because of the implementation of anti-terrorism legislation in the aftermath of recent terrorist attacks; the UK, as the European country at the forefront of expanding government surveillance measures in the name of national security; Germany, because its historical experience with surveillance might lead it to resist the normalisation of surveillance; and, finally the EU, as itself an actor in the context of surveillance.

2 Current state of mass surveillance in Europe

A few years ago, a wave of outrage swept through Europe. The revelations leaked by whistleblower Edward Snowden that the US National Security Agency (NSA) and its Five Eyes partner intelligence services had been conducting mass surveillance that affected their own citizens for years and even targeted the political establishment of many of its allies with their programmes drew widespread anger in many European capitals. However, in 2017 this outrage has become history. The general public in many European states might still be worried about mass surveillance, as discussed in the next section, but their leaders have decided to catch up with the NSA and the UK Government Communications Headquarters

(GCHQ) (the UK's intelligence and security arm) and either extend their own surveillance measures or legalise those already in place.

A report by the EU's Fundamental Rights Agency (FRA) of November 2015 examines how legal frameworks in EU countries enable the use of surveillance techniques, and investigates the role of specialised oversight bodies over intelligence services (with both a foreign and domestic mandate), focusing on the right to privacy and the right to data protection (European Union Agency for Fundamental Rights 2015: 8-9). Not surprisingly, the report finds that the organisation, structure, regulation and oversight of intelligence services differ across the 28 EU member states. The same applies to the concept of national security, which is not harmonised across EU member states, while the scope of the concept is rarely defined (European Union Agency for Fundamental Rights 2015: 27).

Since mass surveillance is not a legal term, the report primarily discusses targeted and untargeted data collection. Targeted surveillance refers to traditional forms of secret data interception, such as phone tapping, and presumes the existence of prior suspicion of a target individual or organisation (European Union Agency for Fundamental Rights 2015: 17). It is also widely known in the legislation of EU member states. With the exception of Cyprus and Portugal, all member states have codified their use of targeted surveillance into law (European Union Agency for Fundamental Rights 2015: 20). Untargeted data collection, on the other hand, is carried out with the type of mass surveillance programmes such as TEMPORA (a codeword for the GCHQ's formerly secret computer programme) and UPSTREAM (the NSA's interception of communications system) that were revealed by Edward Snowden (European Union Agency for Fundamental Rights 2015: 17). Only five EU member states (France, Germany, The Netherlands, Sweden and the UK) have legal frameworks that lay out how intelligence services can use signal intelligence (SIGINT).[1] However, SIGINT legislation in these five countries is also problematic The report states (European Union Agency for Fundamental Rights 2015: 17):

> The Snowden revelations have demonstrated that current legal frameworks and oversight structures have been unable to keep up with technological developments that allow for the collection of vast amounts of data. In some cases, outdated laws not intended to regulate these new forms of surveillance are being used to justify them.

Furthermore, the Council of Europe Commissioner for Human Rights also concludes that 'in many Council of Europe member states, bulk, untargeted surveillance by security services either is not regulated by any publicly available law or regulated in such a nebulous way that the law provides few restraints and little clarity on these measures' (Council of Europe Commissioner for Human Rights 2015: 23). With regard to the oversight of intelligence services, the FRA report also finds that 'a number of EU member states do not provide their external oversight bodies with broad powers, backed by effective independence and means. They

1 The Venice Commission defines signals intelligence as 'a collective term referring to means and methods for the interception and analysis of radio (including satellite and cellular phone) and cable-borne communications' (European Union Agency for Fundamental Rights, 2015, 15)

therefore rely heavily on executive control' (European Union Agency for Fundamental Rights 2015: 34).

The FRA findings, along with various other organisations quoted above, show that surveillance legislation in Europe is in dire need of revision. Judicial oversight has to be vastly improved and legislation amended so that people can understand the reasons and legal framework that allow government surveillance and are able to challenge these.

Already at the time of writing of the FRA report, and particularly in response to the growing number of terrorist attacks on EU soil, governments were starting to put into place legislation that expands the surveillance powers of intelligence and law enforcement authorities. However, instead of including more provisions allowing for adequate judicial oversight and attempting to safeguard human rights, the opposite trend is emerging.

In fact, an Amnesty International report of 2017 on the ever-expanding national security state in Europe found that many EU states now have joined the ranks of 'surveillance' states, and that many European governments justify enhancing their surveillance powers by citing security threats (Amnesty International 2017: 26). Specifically, the report states that '[s]tates have vastly expanded executive power and largely neutralised the ability of the judiciary to serve as a prior check, thus granting the executive virtual monopoly of power over mass surveillance' (Amnesty International 2017: 26). The report investigated counterterrorism legislation in 14 EU countries in depth, and eight of these (Austria, Belgium, France, Germany, Hungary, The Netherlands, Poland and the UK) stand out in the context of government surveillance. The table below focuses on this article's three country examples: France, Germany and the UK.

Country	Legislation	Date	What does it do?	Oversight
France	Law No 2015-912	July 2015	Gives PM power to authorise the use of surveillance measures for wide range of goals. Permits indiscriminate mass surveillance techniques like capturing mobile phone calls and ISP black boxes collecting the personal data of millions of internet users	No prior judicial authorisation required; no ongoing independent judicial oversight

France	Law No 2015-1556	Nov 2015	Allows indiscriminate mass surveillance of all electronic communications (content and metadata) sent to, or received from, abroad (including communications sent from one French citizen to another via servers located abroad)	
	Law No 2016-987 Art 15	July 2016	Law renewing the state of emergency amending the Law on National Security. Gives PM extended surveillance powers over electronic communications regarding individuals suspected of constituting a threat or of 'being associated' with someone who may constitute a threat	No prior judicial authorisation required
Germany	*Gesetz zur Verbesserung der Zusammenarbeit im Bereich des Verfassungsschutzes*	2015	Expands surveillance powers of intelligence service (BND) in response to 'cyber threats'	
	Gesetz zur Ausland-Ausland-Fernmeldeaufklärung des BND	Oct 2016	Permits BND to intercept, collect and process the communications of non-EU citizens outside Germany when the interception point is in Germany (bulk and targeted surveillance) for vague and overly broad goals.	No provision for independent judicial oversight

UK	Investigatory Powers Bill (Snoopers Charter)	Nov 2016	Institutionalises highly intrusive bulk surveillance powers: bulk interception, bulk acquisition, access to bulk personal datasets, bulk hacking – all without any requirement for individualised, reasonable suspicion	Lacks provision for an independent authorisation and oversight mechanism.

All these laws were rushed through parliament, in some cases despite opposition from civil society groups and high-ranking UN officials. Indiscriminate mass surveillance has been denounced by the UN High Commissioner for Human Rights (United Nations Human Rights Council, 30 June 2014), the Special Rapporteur on the Protection of Human Rights while Countering Terrorism (United Nations, 23 September 2014) and the Special Rapporteur on Freedom of Expression (La Rue, 17 April 2013). In 2015, the UN Human Rights Council also established a permanent Special Rapporteur on Privacy, whose tasks include reporting on alleged violations of the right to privacy which arise 'in connection with the challenges arising from new technologies' (United Nations OHCHR).

In Europe, the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE Committee) stated in a report on NSA surveillance programmes that 'the fight against terrorism can never be a justification for untargeted, secret, or even illegal mass surveillances programmes' and 'takes the view that such programmes are incompatible with the principles of necessity and proportionality in a democratic society' (LIBE Committee 2013-2014). The Council of Europe's Commissioner for Human Rights took a similar stand and wrote that secret, massive and indiscriminate surveillance violated European human rights law (Council of Europe Commissioner for Human Rights 2014). In April 2015, the Parliamentary Assembly of the Council of Europe adopted a resolution denouncing surveillance in very strong terms.

The surveillance practices so far disclosed endanger fundamental human rights, including the rights to privacy, freedom of information and expression, and the rights to a fair trial and freedom of religion, especially when the privileged communications of lawyers and religious ministers are intercepted and when digital evidence is manipulated. These rights are the cornerstones of democracy. Their infringement without adequate judicial control also jeopardises the rule of law (Council of Europe Parliamentary Assembly 2015).

In addition to such opposition, European courts have also ruled against mass surveillance. In *Schrems v the Data Protection Commissioner of the Republic of Ireland*, the Court of Justice of the EU concluded that legislation giving the authorities general access to the content of electronic communications compromises the essence of the fundamental right to respect for private life, as guaranteed by article 7 of the EU Charter (*Maximilian Schrems v the Data Protection Commissioner of the Republic of Ireland* 2015: para 94). The European Court of Human Rights condemned

Hungary's unlawful surveillance practices in *Szabo and Vissy v Hungary*, and decided in *Roman Zakharov v Russia* (2015) that the regime in Russia violated Convention rights for the surveillance of telecommunications without prior judicial authorisation based on individual reasonable suspicion of wrongdoing.

However, neither the court decisions nor opposition from the UN and EU have had any significant impact on quelling governments' desire for expanding their use of surveillance measures. Surveillance measures deemed unlawful remain either in place or are implemented, if they do not already exist, always in the name of national security. This trend is disturbing, as is the recurring argument governments use to excuse their surveillance activities by stressing that these measures are not aimed at their own citizens but at threats from outsiders. However, the flow of electronic data makes it increasingly difficult to distinguish between citizens and non-citizens. Furthermore, if all governments engage in mass surveillance, even if not aiming at their own citizens, everyone will remain under surveillance.

The EU itself is also caught up in surveillance controversy. In the name of external border control, the EU has created a vast network of control centres and databases. The European Border Surveillance System (Eurosur) connects the National Co-ordination Centres (NCCs), Frontex, the EU Satellite Centre (SatCen) and the European Maritime Safety Agency (EMSA) and allows for information exchange between EU member states (Frontex 2017). While the Eurosur website states that the information exchanged within Eurosur does not include personal data, Frontex is also linked to the EU-LISA operations centre, which manages the three main information technology systems dealing with visas, asylum requests and the exchange of information to guarantee the security of the Schengen Area (EU-LISA 2017). These databases store records on approximately one million people wanted by the police, 32 million visa applicants, and more than five million asylum seekers (Simantke & Schumann 2016). Across the EU, border guards can access this data when examing travellers, with three more databases on airline passengers and travellers from non-EU states soon joining the existing bases (Simantke & Schumann 2016).

Although investigative journalists and French parliamentarians have found that much of Eurosur's information exchange is largely hypothetical and, in practice, does not do much to help the external border agencies on the ground, the mere installation of these systems shows how powerful the concept of ensuring security is in the minds of EU officials (Simantke & Schumann 2016). Since the 9/11 attacks, the EU has channelled billions of euros into research programmes in order 'to develop an autonomous security industry which did not exist before' (Simantke & Schumann 2016). Between 2004 and 2014, 360 million euros of tax money went into new technologies for border surveillance alone: 'The spectrum ranges from high-tech drones for remote monitoring to document scanners with database connection, from networking software for security authorities to the integration of data streams in situational pictures' (Simantke & Schumann 2016). This has led to a symbiotic relationship with the security industry, conflicts of interest for EU officials, and the security industry deciding what constitutes 'security' (Simantke & Schumann 2016). The consequence, according to security scholar Peter Burgess, is that the focus is always on surveillance technology, even though 'there is

very little evidence that it works' (Simantke & Schumann 2016). Despite Eurosur's problems, EU officials remain unrelenting by dismissing criticism and defending their policy line that more surveillance technology and data collection equal more security (Simantke & Schumann 2016). Yet, whether these technologies actually increase security is something that is not publicly discussed, let alone evaluated.

The lack of evaluation and even discussion of surveillance measures, of course, in large part is due to the secretive nature of government surveillance. The public has to rely on the information the government deems safe to disclose, but often stages its lack of surveillance transparency as a matter of security. Decision making surrounding surveillance operations, thus, occurs away from the public eye, which favours securitisation. The next section examines in more detail the relationship between public opinion and surveillance.

3 Complicit public?

Audience is a key concept in securitisation theory. According to Buzan et al, an issue can only be considered securitised if and when the audience accepts it as securitised (Buzan et al 1998: 25). As a result, securitisation scholars have tried to answer many questions surrounding the topic of audience acceptance, but criteria for what constitutes audience acceptance nevertheless remain vague (Balzacq et al 2015: 499). When it comes to surveillance, the question of audience acceptance is equally important. Although surveillance is not a securitised issue, it is a necessary tool to fight the existential threat of terrorism, at least that is how governments justify the use of surveillance. This, then, makes surveillance an important aspect of current securitisation processes in Europe, while at the same time raising interesting questions about the audience acceptance of counterterrorism measures itself.

Balzacq et al summarise the view of the audience among securitisation scholars (Balzacq et al 2015: 500):

> The audience does more than merely sanctioning a securitising move. The audience can actually fulfil two different functions, namely, providing moral support and supplying the securitising actor with a formal mandate (such as a vote by the legislature), without which no policy to address the threat would be possible.

The example they cite is the decision of the British government to invade Iraq in 2003. Prime Minister Tony Blair's decision did not have the moral support of the public, but it did garner formal agreement from parliament, which constitutes another audience (Balzacq et al 2015: 500). A similar dynamic can be observed when it comes to government decisions to employ mass surveillance tools. As the current wave of legislative measures to allow governments to use mass surveillance technologies outlined in the previous section shows, executive branches are successful in persuading parliaments to pass such laws. The public attitude towards surveillance programmes, however, is more nuanced.

A report from November 2015 analysing public attitudes in the EU and the UK towards surveillance, privacy and security post-Snowden found that citizens are concerned about surveillance (Bakir et al 2015).[2] While most of the people surveyed in the EU agree or strongly agree that

security-oriented surveillance technologies are effective national security tools, the EU public also consider all these technologies to compromise human rights and to be abused by security agencies (Bakir et al 2015: 9). The report also shows that, on the whole, the public in the EU does not accept blanket mass surveillance and finds technologies used for such surveillance significantly less acceptable than those focusing on specific targets (Bakir et al 2015: 10). Furthermore, the polls show that the public wants enforced and increased accountability, liability and transparency of private and state surveillance actors (Bakir et al 2015: 10).

These findings underline public concerns about surveillance, but they also hint at the difficult question of how to reconcile concerns over security with concerns over privacy in the context of surveillance. Two Eurobarometer polls from 2015 also underline these competing interests in public opinion. Eurobarometer 432 on Europeans' attitude on security demonstrates that there is rising concern about terrorism and religious extremism to the point where people now see terrorism as the EU's most important security challenge (European Union 2015b). While in 2011 less than half the respondents said that citizens' rights and freedoms had been restricted in the name of fighting terrorism and crime, the majority of respondents felt that way in 2015 (European Union 2015b: 53). Eurobarometer 431 was conducted at the same time as Eurobarometer 432 and highlights people's concerns about data protection and privacy. The poll found that only 15 per cent of respondents felt that they had complete control over the information they provide online; and 31 per cent thought that they had no control over it at all (European Union 2015a: 6). Fifty-five percent of respondents also said that they were concerned about the recording of their activities via mobile phones (European Union 2015a: 6).

These responses show that the public is aware of the fact that their rights are infringed, either to provide security from terrorism and crime or because there are not enough data protection measures in place. And yet, public outrage over an increase in recent legislation to allow governments to access even more data has been muted. This begs the question why. One argument is that in the wake of more terrorist attacks across Europe, fear has risen and people's willingness to sacrifice human rights in the name of security has increased along with it.

A YouGov poll comparing the attitudes in seven European countries (Great Britain, Germany, France, Denmark, Sweden, Finland and Norway) shows that about half of the respondents in all of these countries except Germany agree that '[t]he security forces should be given more investigative powers to combat terrorism, even if this means the privacy or human rights of ordinary people suffers': 52 per cent in Great Britain; 50 per cent in France; 41 per cent in Denmark; 44 per cent in Sweden and Finland; and 43 per cent in Norway (Germans resist push for greater government spying March 2015). Only respondents from Germany were more skeptical about investigative powers: 31 per cent agreed with the above statement, while 27 per cent said that '[m]ore should be done to protect the privacy and human rights of ordinary people, even if this puts some limits on what the security forces can do when combating terrorism' (Germans resist push for greater government spying March 2015). In

2 The report summarises several public opinion polls conducted in the EU and across the UK.

Great Britain, 16 per cent of respondents agreed with this statement; 19 per cent in France; 17 per cent in Denmark; 21 per cent in Sweden; 13 per cent in Finland; and 18 per cent in Norway (Germans resist push for greater government spying March 2015). When asked whether security services should or should not be allowed to store the details (but not the actual contents) of ordinary people's communications, such as email and mobile phone calls, the same trends emerged. In Great Britain, 50 per cent of respondents said that it should be allowed, while 52 per cent in Denmark, 53 per cent in Sweden, and even 61 per cent in France agreed. In Germany and Finland, only 34 per cent of respondents said that it should be allowed (Germans resist push for greater government spying March 2015).

These polls show that people tend to favour security measures even if these come at the expense of human rights and privacy, and thus makes the public to a large degree complicit in their governments' legislation and implementation of surveillance measures. However, when it comes to surveillance, there are also other factors that lead the public to be complicit in the governments' accumulation of more surveillance powers. In Eurobarometer 431, a large majority of people (71 per cent) said that providing personal information was an increasing part of modern life, and accepted that there is no alternative other than to provide it if they want to obtain products or services (European Union 2015a: 6). This shows that people do not in this day and age see a way around providing personal information online. The comparative study also concludes that 'state surveillance is being carried out on the basis of public resignation rather than apathy or consent' (Bakir et al 2015: 8).

Similarly, a more recent study which examines public opinion and activist responses to the Snowden leaks, argues that public opinion on surveillance and online privacy is characterised by 'surveillance realism' (Dencik & Cable 2017: 763). This condition, they contend, is a result of the lack of transparency, knowledge and control over what happens to personal data online, which in turn causes feelings of widespread resignation, not consent, to the status quo (Dencik & Cable 2017: 763). Surveillance realism thus is characterised by citizens' unease with data collection and by active normalisation of surveillance that leads to feelings of disempowerment among the public and a lack of imagination for better alternatives to safeguard human rights while employing surveillance technologies (Dencik & Cable 2017: 778). In short, the popular feeling of resignation in the face of mass surveillance technologies undermines democracy, as government policies implementing mass surveillance are not established by the consent of the citizenry.

A large-scale, EU-financed research project on surveillance technology and its ethics and efficiency includes an in-depth analysis of the public perceptions of surveillance and their effects. The main findings are summarised in the table below. The first column lists the various sources of negative public perceptions of surveillance. The second point, security dilemma and surveillance spiral, is particularly interesting given some of the public opinion poll results cited above, and the concern of this article with permanent securitisation. The security dilemma refers to security technologies increasing people's feelings of insecurity rather than making them feel safer (Orru et al 2013 14). For example, some studies show that people are more anxious about crime in areas where closed-circuit

television cameras are installed (Orru et al 2013: 14). This, then, can lead to a surveillance spiral, because if people feel less safe, there is a need for more surveillance (Orru et al 2013: 14). In turn, this might lead to governments gaining even more surveillance powers in the name of security, which might further create an environment for permanent securitisation.

Potential sources of negative perception:	**Potential consequences of negative perception:**	**Impact on society:**
Technologies perceived as threats themselves Security dilemma and surveillance spiral Fear of misuse (including function creep) Fear of insufficient protection of personal data Fear of unlimited expansion and irreversibility	Self-surveillance Chilling effect (eg by stifling online expression) Conformism and loss of autonomy	Control society Social exclusion and discrimination Social homogenisation Decline of solidarity

In the third column, the table lists the side effects of the negative perceptions of surveillance such as control society, social exclusion and discrimination, social homogenisation, and a decline of solidarity. Some of these can already be observed in the democracies of the EU, and all of them are stepping stones for governments to extend their powers. What is more, these findings show that fear of surveillance can be just as powerful and detrimental as surveillance itself.

The effects of the negative perceptions of surveillance along with surveillance realism also highlight the importance of the public role in accepting the implementation of mass surveillance technologies and creating a climate for permanent securitisation. On the one hand, the public distrusts surveillance and intelligence services. On the other, they feel disempowered to change anything.

The rise of populists in many European countries further complicates this situation. Many of these populist parties, especially those with an anti-EU stance, complain about how technocrats allegedly have too much power over policies. They say that they want to give their country back to the people. At the same time, however, they swear that they are committed to fighting terrorism and that they are tough on the terrorists, which implies an increased reliance on the surveillance apparatus. This seems contradictory. They seem to be saying that they will curtail the powers of the EU and the elites, but at the same time they seem to say that they will curtail individual rights in the name of security.

The slogan for the 'Leave' campaign in the run-up to the Brexit vote was 'Take Back Control'. The result of the vote showed that this sentiment of taking back control resonated with many voters. In fact, the EU is now trying to appropriate the 'Take Back Control' slogan for its own purposes (Heath 2016). However, looking at the example of public opinion towards surveillance, there seems to be a disconnect between taking back political control over one's country versus control over one's political rights. In

order to take back political control, however, civil and political rights in the first place have to be secured. Disturbingly, mass surveillance erodes these rights. Furthermore, if mass surveillance tools are permanently installed as vital instruments to ensure security, in this case because of public resignation rather than consent, we are also moving one step closer to permanent securitisation.

4 Impact of mass surveillance on human rights

Mass surveillance has an impact on human rights in various ways. The primary rights affected by mass surveillance are the right to privacy and the right to data protection. However, other rights, such as freedom of expression, freedom of information, freedom of the press, freedom of association and freedom of assembly, are also impacted by mass surveillance. To address all these in detail would exceed the scope of this article. Instead, the article will focus on how mass surveillance undermines human rights and democracy overall. These rights are indivisible and closely connected to democratic politics and society, and thus garner a holistic approach, one that incidentally tends to be overlooked when it comes to the threat of mass surveillance and its relationship to permanent securitisation.

The right to privacy ensures self-expression and personal autonomy, which are vital for self-determination. However, surveillance undermines these freedoms. People who are watched or who think that they are being watched behave differently from their unwatched selves; they exercise self-control and self-censorship. The resulting society is a control society, in which people try to conform out of fear of showing their true selves and intentions because the government holds vastly more power than they do.

Surveillance, or fear of surveillance, also leads to an erosion of trust. Evidence of this can be seen in the result of the public opinion polls listed above that show that a majority of respondents think that government agencies abuse their surveillance powers. As argued in the previous section, this leads to resignation and unease among citizens and inhibits their civic engagement. What is more, you cannot take political action if you have no privacy. Brad Smith, the president and chief legal advisor of Microsoft, summed it up at a recent conference on liberty in the digital age: 'If you can't plan in private, you can't act in public.'

All this runs counter to the idea of democracy, in which the people are in control of their governments. Surveillance, therefore, has an impact on state-society relations as a whole. This, however, is often overlooked, even in the human rights community, because, as Cas et al state: 'Most privacy-surveillance problems lack dead bodies and sensationalistic cases' such as blacklists (Cas et al 2014: 223).

Yet, the implications of mass surveillance on state-society relations are detrimental. Mass surveillance tips the scales of power towards the governments. In the words of Snowden (Snowden and Bell 2017: 57):

> It's not really about surveillance; it's about what the public understands – how much control the public has over the programs and policies of its governments. If we don't know what our government really does, if we don't know the powers that authorities are claiming for themselves, or arrogating

> to themselves, in secret, we can't really be said to be holding the leash of government at all.

Current mass surveillance practices, therefore, are extremely dangerous to human rights and democratic society and politics, and there is no shortage of recent examples of how mass surveillance legislation undermines civil society, particularly human rights defenders and journalists. In Germany, the new *Bundesnachrichtendienst* (BND) law allows the intelligence service to spy on foreign journalists, a practice that the BND has been engaging in for years already by spying on journalists from the BBC, *New York Times*, Reuters, and other news organisations (Baumgärtner et al 2017). Furthermore, the so-called *Datenhehlerei* paragraph in a 2015 enacted law on data retention criminalises the handling of stolen data, troubling journalists and transparency non-governmental organisations (NGOs) that it will intimidate whistleblowers (Freedom House 2017a).

In the UK, it emerged that Amnesty International had been under surveillance by the British intelligence services, who intercepted, accessed and stored the organisation's communications, prompting the organisation to ask: 'How can we be expected to carry out our crucial work around the world if human rights defenders and victims of abuses can now credibly believe their confidential correspondence with us is likely to end up in the hands of governments?' (Amnesty International 2015). Moreover, British police have admitted that they used surveillance legislation in order to obtain journalistic material, bypassing other laws that require special warrants for journalists' records (Freedom House 2017b).

In France, the recently legalised mass surveillance powers have been met with similar criticism as those in Germany. As one French journalist put it: 'Now you have to meet your sources somewhere in a forest with a pen and a piece of paper to avoid surveillance which is not always possible' (European Federation of Journalists 2016). In Hungary, the government is taking things even further, with law makers discussing national security legislation that would allow state intelligence agents to be stationed inside newsrooms (Intelligence agents could be stationed in newsrooms 2015).

These examples clearly show that governments are not simply using mass surveillance to counter terrorism. On the contrary, they are using their surveillance powers to undermine civil society and their most prominent defenders: journalists and human rights organisations. Civil society is vital to mobilise against government policies and challenge the dominant political discourse focused on national security. This means that if civil society weakens, the way is open for governments to implement ever more illiberal policies in the name of security. Hungary, where independent media and NGOs have been undermined for years now, serves as a cautionary tale. Political debate has become so one-sided to the point where government-critical voices gain little to no public exposure. However, Hungary is not an isolated case. The same forces are moving to undermine human rights and democracy all across the continent.

5 Mass surveillance and permanent securitisation

The previous sections have highlighted several ways in which the implementation of mass surveillance drives permanent securitisation. Negative public perceptions of surveillance lead to negative effects on

individuals and society. The ubiquity of surveillance and the secrecy surrounding it create resignation and political passivity among the citizenry, which undermines informed consent and, ultimately, democracy. Together, these factors create an environment in which securitising actors can push for ever more policies that emphasise security at the expense of human rights.

When it comes to protecting human rights, the use of mass surveillance creates a vicious cycle: Security threats require mass surveillance; mass surveillance undermines human rights, especially those of human rights defenders and journalists, who are vital for civil society. In turn, the erosion of civil society leads to a lack of public debate and, thus, a lack of policies curtailing mass surveillance and securitisation. This gives the government more leeway to introduce even more legislation that undermines human rights in the name of protecting people from security threats.

In this context, it is worth highlighting that scholars of the so-called Paris School have argued that securitisation does not simply occur as a result of speech acts. Securitisation, they point out, is not necessarily the result of rational design and preordained agendas (Balzacq 2011: 16). In order to identify the processes of securitisation, they argue, it is important to take into account security practices and study the instruments or tools that are employed to cope with security issues and that can lead to the routinisation of practices (Balzacq 2011: 16-17). As demonstrated throughout this article, surveillance measures are instruments used by governments in the context of countering terrorism and managing migration. They become routinised through their use by security professionals, who may not be too concerned with legal frameworks, but rather with carrying out their duties. Furthermore, once these instruments have been implemented, their use might lead to function or mission creep. First, a new technology is used to fight terrorists, then to catch criminals or other offenders, and then for even other potential purposes that the original implementers did not intend or foresee. In sum, the use of these technologies can take on a life of its own if not overseen properly, and once they are implemented, it is difficult to reverse them.

It is also worth keeping in mind in this context that studies have shown that securitisation can happen through the most ordinary steps. Even policies that seem exceptional are often established through the most banal laws (Balzacq et al 2015: 506). In order to guard against creeping securitisation, therefore, it is not enough to simply point at democratic governments that are turning to illiberal policies, such as Hungary and Poland, as cautionary tales. It is important to be aware that securitisation processes also happen within the framework of liberal legislation, especially in the current political climate across Europe, which is dominated by national security issues.

As the examples in this article show, liberal regimes have already been successful in legalising previously unlawful surveillance practices, and many others in Europe are in the process of doing so. In *Surveillance in Europe,* published in 2014, observers already remarked that '[f]requently, rather than law determining the use of the technology, law is reactive and often legitimises current practices rather than shaping practice based on a principled approach' (Kreissl et al 2014: 154). Following the 2015 and subsequent terrorist attacks in Europe, this statement rings even truer

today. In an in-depth study tracing recent surveillance legislation in France, the author argues that due to renewed securitisation rhetoric on Islamic terrorism following the attacks, the French government was able to legalise previously illegal surveillance practices (Treguer 2016). The government, he contends, moved away from the 'rule *of* law' towards the 'rule *by* law' (Treguer 2016: 7). As Tarrow (2015: 165-166) points out, this is an important distinction to make:

> Is the distinction between rule of law and rule by law a distinction without difference? I think not. First, rule by law convinces both decision makers and operatives that their illegal behavior is legally protected … Second, engaging in rule by law provides a defense against the charge they are breaking the law. Over time, and repeated often enough, this can create a 'new normal'.

Again, this brings us back to the problem of normalisation of both surveillance and securitisation, which threatens to permanently undermine civil liberties and democracy in favour of security. How dangerously close we already are to drifting into a permanent state of securitisation is demonstrated by human rights defenders working on the issue of counterterrorism and its implications for human rights, being resigned about the fact that their alarming reports and findings are not garnering any public attention. Indeed, there is practically no public debate about whether mass surveillance even works in preventing terrorism. In fact, so far there is very little evidence that it does (Kirchner 2015). A 2013 US government report concludes that the NSA's bulk collection of phone records 'was not essential to preventing attacks', and local police departments in the US have also acknowledged the limits of mass surveillance (Kirchner 2015). Some go even further, arguing that electronic mass surveillance can hinder counterterrorism efforts because, instead of conducting targeted monitoring, intelligence analysts are wasting their time fruitlessly sifting through vast amounts of data (Noakes 2016). Additionally, counter-radicalisation experts argue that mass surveillance may alienate Muslim communities and contribute to radicalisation (Noakes 2016).

Other observers have pointed out that new surveillance technologies are often introduced without any prior evaluation or assessment (Kreissl et al 2014: 154). The problem in this context is that the public is in the weaker position in terms of evaluating whether these technologies are really necessary because they have to rely on the information presented by intelligence services and law enforcement (Kreissl et al 2014: 155). The cross-disciplinary collaborative research project SURVEILLE, funded by the European Commission, created a methodology to determine on a case by case basis whether it is legal, moral, efficient, and effective to use a particular surveillance technology (SURVEILLE 2015). In their policy paper summary, the researchers conclude that 'the SURVEILLE methodology shows that it is possible to reconcile security and privacy in a rational and structured way' (SURVEILLE 2015). Whether this methodology is actually used by technology developers, law makers and security professionals, however, remains doubtful.

6 Way forward

As this article shows, mass surveillance is now widely regarded by policy and law makers as well as by large parts of the public as a necessary tool to

counter terrorism. However, the efficiency of mass surveillance tools as well as the dangers they pose for human rights and democracy is not adequately addressed in the public debate. Instead, the normalisation of mass surveillance goes hand in hand with creating a permanent state of securitisation in Europe, where security has become the dominant policy paradigm. Given this shift towards permanent securitisation at the expense of civil and political rights as well as democratic structures as a whole, it is vital for the human rights community to find a way to counter these developments.

Warnings about the dangers of surveillance states are not new, of course, and since the Snowden revelations in 2013 they have increased at the civil society level as well as at the level of regional and international human rights bodies. Yet, the public debate on mass surveillance remains fairly one-sided, with governments dominating the agenda by justifying their use of mass surveillance with counterterrorism measures and protecting the public. Researchers (Wright & Kreissl 2014; IRISS Consortium 2014) have called for increasing resilience in surveillance societies and have come to similar conclusions on what is needed to equip societies in order to cope with an increased level of surveillance. At the political and regulatory level, it is vital to establish better accountability and oversight procedures as well as improving legal and constitutional protection of privacy (Wright & Kreissl 2014; IRISS Consortium 2014). As evidence in this article shows, however, law makers across Europe are currently busy legalising executive surveillance powers without adequate accountability or oversight mechanisms in place.

At the individual level, these studies call for instilling resilient attitudes and the increased use of privacy-enhancing technologies (IRISS Consortium 2014: 31-34). However, here too the evidence paints a rather bleak picture, as many people in European countries feel disempowered in light of the ubiquity of surveillance technology in the twenty-first century that seems to make it unavoidable to guard privacy and human rights. This leaves resilience at societal level, which requires strong collective action and civil society organisations as well as an independent, activist press to stir public debate towards a more critical approach to mass surveillance and securitisation in general. Civil society, however, is in decline and the press is under unprecedented attack in many European countries, not least due to increased surveillance measures.

Given these circumstances, resilience to both surveillance and securitisation poses a difficult challenge. In order to forge ahead and implement the steps laid out by the resilience studies, what is required first is a re-evaluation of narratives and, what is more, the creation of powerful counter-narratives that can challenge the current securitisation discourses and highlight the relevance of human rights and democracy. Human security is useful in this context in that it focuses on the individual at the centre of the concept of security, rather than on the security of the state, which is the predominant notion in the ongoing counterterrorism policies of European countries. It is, however, a less useful concept in addressing the issue of surveillance.

Stressing the idea of popular sovereignty might also prove useful in this context. For all the talk by various populist parties across Europe, there is little focus on the notion of *popular* sovereignty. What has gotten lost in the many discourses that emphasise the many threats to our security,

Europeans seem to have lost sight of the fundamental concept on which human rights and democracy rest: the notion that the people are the masters of their governments. Europeans forget or take this idea for granted, while governments everywhere are expanding their power over their people, while ensuring them that they are doing this because people's security is at stake. By being silent in the wake of ever-expanding government surveillance, the public becomes weaker and weaker vis-à-vis governments, thus moving away further from the ideal of popular sovereignty. However, the concept of popular sovereignty has been linked to nationalism in the past and, given the nationalist resurgence in Europe in recent years, it might be difficult to disentangle the very valuable idea of the people as the masters of their government from those sovereignty concepts that are appropriated by nationalists.

What then, can be done in terms of creating relevant, powerful anti-surveillance, anti-securitisation, pro-human rights and pro-democracy narratives? Securitisation scholar Didier Bigo argues in an analysis of the EU's 2005 Hague Programme on strengthening freedom, security and justice in the European Union that 'just as security has to be understood as a process of securitisation/insecuritisation/desecuritisation, so has freedom to be understood as a process of freedomisation/unfreedomisation and defreedomisation' (Bigo 2006: 38). The answer, thus, lies in re-focusing on the idea of freedom: What does it mean to be free in the twenty-first century, in the digital age, in an age of increased terror attacks on European soil? What are the values that are non-negotiable when it comes to weighing the risk of curtailing privacy and human rights against security? Further research is required into how to create positive human rights narratives that are able to counter the narratives of securitisation and that will keep us from drifting further into permanent states of surveillance and securitisation. However, it is a useful start to focus on the concept of freedom, and thinking about what we are trying to secure in Europe in the first place.

References

Amnesty International *UK surveillance Tribunal reveals the government spied on Amnesty International*, 1 July 2015, available at https://www.amnesty.org/en/latest/news/2015/07/uk-surveillance-tribunal-reveals-the-government-spied-on-amnesty-international/ (last visited 5 May 2017)

Amnesty International (2017) *Dangerously disproportionate: The ever-expanding national security state in Europe* London: Amnesty International

Bakir V, Cable J, Dencik L, Hintz A & McStay 'A public feeling on privacy, security and surveillance: A report by DATA-PSST and DCSS', November 2015, available at https://sites.cardiff.ac.uk/dcssproject/files/2015/11/Public-Feeling-on-Privacy-Security-Surveillance-DATAPSST-DCSS-Nov2015.pdf (last visited 5 May 2017)

Balzacq T 'A theory of securitization: origins, core assumptions, and variants' in T Balzacq (ed) *Securitization theory: How security problems emerge and* dissolve (2011) London: Routledge

Balzacq T, Leonard S & Ruzicka J '"Securitization" revisited: Theory and cases' (2015) 30 *International Relations* 494

Baumgärtner M, Knobbe M & Schindler J 'Documents indicate Germany spied on foreign journalists' *Spiegel Online* 24 February 2017, available at http://www.spiegel.de/international/germany/german-intelligence-spied-on-foreign-journalists-for-years-a-1136188.html (last visited 5 May 2017)

Bigo D 'Liberty, whose liberty? The Hague Programme and the conception of freedom' in T Balzacq & S Carrera (eds) *Security versus freedom? A challenge for Europe's future* ((2006) Aldershot: Ashgate

Buzan B, Waever O & De Wilde J (1998) *Security: A new framework for analysis* Boulder, London: Lynne Rienner Publishers

Cas J, Strauss S, Amicelle A, Ball K, Halliman D, Friedewald M & Szekely I 'Social and economic costs of surveillance' in D Wright & R Kreissl (eds) (2014) *Surveillance in Europe* London: Routledge

Council of Europe Commissioner for Human Rights Issue Paper: 'Democratic and effective oversight of national security services' Strasbourg: Council of Europe (2015)

Council of Europe Commissioner for Human Rights 'The rule of law on the internet and in the wider digital world' December 2014 Council of Europe

Council of Europe Parliamentary Assembly *Resolution 2045 (2015): Mass Surveillance* 2015, available at http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=21692&lang=en (last visited 5 May 2017)

Dencik L & Cable J 'The advent of surveillance realism: Public opinion and activist responses to the Snowden leaks' (2017) 11 *International Journal of Communication* 763

EU-LISA *Operational Management*, 2017, available at http://www.eulisa.europa.eu/AboutUs/MandateAndActivities/CoreActivities/Pages/OperationalManagement.aspx (last visited 5 May 2017)

European Federation of Journalists *Self-censorship is affecting more and more European media* 2 May 2016, available at http://europeanjournalists.org/blog/2016/05/02/self-censorship-is-affecting-more-and-more-european-media/ (last visiteed 5 May 2017)

European Union 'Special Eurobarometer 431: Data protection' (2015a), available at http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_431_en.pdf (last visited 5 May 2017)

European Union 'Special Eurobarometer 432: Europeans' attitudes towards security' (2015b) available at http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_432_en.pdf (last visited 5 May 2017)

European Union Agency for Fundamental Rights *Surveillance by intelligence services: Fundamental rights safeguards and remedies in the EU: Mapping member states' legal frameworks* (2015) Luxembourg: Publications Office of the European Union

Farmer B 'Theresa May: New surveillance powers "question of life and death"' *The Telegraph* 24 June 2014, available at http://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/10923624/Theresa-May-New-surveillance-powers-question-of-life-and-death.html (last visited 5 May 2017)

Freedom House *Germany: Freedom of the press 2016* (2017a), available at https://freedomhouse.org/report/freedom-press/2016/germany (last visited 5 May 2017)

Freedom House *United Kingdom: Freedom of the press 2016* (2017b), available at https://freedomhouse.org/report/freedom-press/2016/united-kingdom (last visited 5 May 2017)

Frontex *EUROSUR* (2017), available at http://frontex.europa.eu/intelligence/eurosur/ (last visited 5 May 2017)

'Germans resist push for greater government spying' *YouGov.co.uk* March 2015, available at https://yougov.co.uk/news/2015/03/05/germans-resist-push-greater-government-surveillanc/ (last visited 5 May 2017)

Heath R Donald 'Tusk pushes "road map" for EU future' *Politico* 12 September 2016, available at http://www.politico.eu/article/european-council-president-donald-tusk-pushes-road-map-for-eu-future-bratislava-summit/ (last visited 5 May 2017)

'Intelligence agents could be stationed in newsrooms' *Budapest Business Journal* 4 November 2015, available at https://bbj.hu/politics/intelligence-agents-could-be-stationed-in-newsrooms_106652 (last visited 5 May 2017)

IRISS Consortium *Handbook on increasing resilience in a surveillance society: Key considerations for policy-makers, regulators, consultancies, service providers, the media, civil society organisations and the public* IRISS Project: EC Grant Agreement No 290492 September 2014

Kirchner L 'What's the evidence mass surveillance works? Not much' *ProPublica* 18 November 2015, available at https://www.propublica.org/article/whats-the-evidence-mass-surveillance-works-not-much (last visited 5 May 2017)

Kreissl R, Norris C, Krlic M, Groves L & Amicelle A (2014) 'Surveillance: Preventing and detecting crime and terrorism' in D Wright & R Kreissl (eds) *Surveillance in Europe* (2014) London: Routledge

La Rue F Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression A/HRC/23/40 17 April 2013, available at http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf (last visited 5 May 2017)

LIBE Committee Inquiry on Electronic Mass Surveillance of EU Citizens: Protecting Fundamental Rights in a Digital Age 2013-2014 European Parliament

Maximilian Schrems v the Data Protection Commissioner of the Republic of Ireland 6 October 2015, C-362/14, Court of Justice of the European Union

Noakes A 'Mass surveillance doesn't work – It's time to go back to the drawing board' *NewStatesman.com* 11 February 2016, available at http://www.newstatesman.com/politics/staggers/2016/02/mass-surveillance-doesn-t-work-it-s-time-go-back-drawing-board (last visited 5 May 2017)

Orru E, Gander H-H & Hoehn S SURVEILLE Deliverable 3.2: Review of European level studies on perceptions of surveillance: Negative perception, effects, side effects and perceived effectiveness *FP7* - SURVEILLE (2013)

Roman Szaharov v Russia 4 December 2015, 47143/06, European Court of Human Rights

Simantke E & Schumann H 'Surveillance without limits – How Europe creates a dysfunctional border regime' *Investigate Europe* 22 December 2016, *a*vailable at http://www.investigate-europe.eu/en/surveillance-without-limits-how-europe-creates-a-dysfunctional-border-regime/ (last visited 5 May 2017)

Snowden E & Bell E 'A conversation with Edward Snowden' in E Bell & T Owen (eds) *Journalism after Snowden: The future of the free press in the surveillance state* (2017) New York: Columbia University Press

SURVEILLE *SURVEILLE Policy Brief: Assessing surveillance technologies: A nuanced approach for determining security benefits against financial costs, moral hazards and impact on fundamental rights* 2015, available at https://surveille.eui.eu/wp-content/uploads/sites/19/2015/07/SURVEILLE-Policy-Brief.pdf (last visited 5 May 2017)

Szabo and Vissy v Hungary 12 January 2016, 37138/14, European Court of Human Rights

Tarrow S (2015) *War, states, and contention: A comparative historical study* Ithaca, NY: Cornell University Press

Treguer F 'From deep state illegality to law of the land: The case of internet surveillance in France' 7th Biennial Surveillance & Society Conference (SSN 2016): *Power, Performance and Trust* Barcelona, Spain 2016

United Nations 'Promotion and protection of human rights and fundamental freedoms while countering terrorism – Note by the Secretary-General' A/69/397 23 September 2014, available at https://documents-dds-ny.un.org/doc/UNDOC/GEN/N14/545/19/PDF/N1454519.pdf?OpenElement (last visited 5 May 2017)

United Nations Human Rights Council The right to privacy in the digital age – Report of the Office of the United Nations High Commissioner for Human Rights A/HRC/27/37 30 June 2014, available at http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf (last visited 5 May 2017)

United Nations OHCHR *Special Rapporteur on the Right to Privacy*, available at http://www.ohchr.org/EN/Issues/Privacy/SR/Pages/SRPrivacyIndex.aspx (last visited 5 May 2017)

Wright D & Kreissl R 'Resilience in Europe's surveillance society' in D Wright & R Kreissl (eds) *Surveillance in Europe* (2014) London: Routledge