The *fifth freedom* and the burden of executive power

Kristrún Gunnarsdóttir [1]

This is a draft version of a book chapter by the same title, in A. Delgado (ed) (2016). *Technoscience and Citizenship: Ethics and Governance of Emerging Technologies*. *The International Library of Ethics, Law and Technology*, Springer Verlag (Ch. 6, Part 3, Governing Citizen's Movements).

A much longer and simpler version of this draft was originally prepared for Spanish non-academic audience.

Abstract. Advanced ICTs and biometry in mass-surveillance and border control is integral to the *securitization agenda* which emerged in the early 2000s. This agenda has been particularly instrumental in cultivating migration anxieties and framing the problem of *threat* as an imperative to identify those who are dangerous to public safety. As well founded as that may be, this framing masks the pivotal role ICTs have in the supervision and surveillance of industries and markets. ICTs are essential to achieve all four freedoms of movement in European market integration, i.e., of *goods*, *services*, *capital* and *persons*. They are essential to EU-US trade and investment relations which are increasingly underpinned by cross-border data flows. Drawing on mobilities research, this chapter explores how the mobilities of materials, commodities, markets and labour are simultaneously constrained and facilitated in reference to the obligation in Europe to protect yet another freedom of movement, that of *data*. Against efforts to better protect personal data in these flows, narratives of threat and emergency call for immediate action, whereby any data that *can* be intercepted can also be gathered for investigative purposes on the basis of *exceptional circumstance*. The securitization agenda finds its practical utility here in the hands of executive powers, avoiding the legislature and the judiciary. There is no evidence that authorities catch terrorists and criminals *because of* advanced ICTs in data intercept. The practical utility lies in the ability to target and investigate any individual, any political opposition or exercise in citizen rights to challenge the socio-economic and moral order. Under the circumstances, the only immediate defence available is self-censorship. Publics have no meaningful way of objecting to states of exception in which illiberal practices are legitimized, and neither does the legislature and the judiciary unless the checks on executive powers are adequately reined in.

1 Sociology Department, Lancaster University, UK, LA1 4YN, Lancaster, UK. Email: k.gunnarsdottir@lancaster.ac.uk

1. Instrumentality and practical utility [2]

Security is the watchword with which to refer to public safety and the safeguarding of first-world economies, markets, democracy and *our* mobile lives. The growth of industries and markets since the second world war coincides with new freedoms of movement, now protected across the Single Market of the European Economic Area (EEA) and in market relations with the United States and beyond. The sustainability of such freedoms is increasingly at issue however. Evidence of political dissidence and hostility toward the socio-economic order and the leadership of first-world democracies and corporate enterprise, give rise to insecurities for which *securitization* has become the all-round remedy.

This chapter addresses a set of issues that tie together securitization objectives in reference to industries and markets, economic leadership and the mobilities afforded by European integration and associated transnational developments. The EEA protects the free movement of goods, services, capital and persons (European Parliament Fact Sheets 2000). Among other things, it supports the abolition of customs duties on industrial goods, the free movement of financial services, telecommunication, information, media services, transport and energy, the freedom of ownership and right to take up residence and employment in any of the EU/EEA member states without visa formalities. Accordingly, the supervision of cross-border mobilities in Europe falls on shared regulatory provisions, including the bureaucratic and technical oversight of EU/EEA and Schengen agreements in these matters.[3]

As regards alliances beyond Europe however, European states have tacitly accepted the leadership of the United States in economic, political and military affairs, with relations stretching further afield tainted by a history of colonialism and exploitation. Calls for democracy on behalf of some of those *others*, come typically on the back of coercive economic and market practices, instigated and policed by the US and former European empires (e.g. Dalacoura 2005; Carothers 2003). While conditions like that give rise to grave concerns over lasting social, economic and territorial discord, hence questions of adequacy with respect to *our leadership*, transnational partnerships are adapting to signs of change. But, as the official argument goes, first-world leadership will have to remake itself in an era of new economic powers, and "[t]hat begins with our economic leadership" (Obama 2011).[4] With that in mind, the most significant trade and investment relationship globally is the one between European states and the US, a relationship increasingly underpinned by cross-border flows of data (Meltzer 2014).

This chapter takes as a point of departure that the proliferation of advanced information and communication technologies (ICTs) in mobility control and surveillance, has very publicly served preoccupations with imminent threat of illicit migration and acts of crime and terror. It argues that such preoccupations, regardless of how well founded they may be, mask the pivotal role ICTs have in the practical supervision and oversight of transnational markets, industry and finance, and they ignore how much of the threat might be rooted in colonial history and first-world leadership. The following sections discuss the question of cohesion in transnational development against the underpinnings of markets in data flows and ICT-based innovation, and how to move away from instrumentalizing the securitization agenda to a point where publics have no meaningful way of challenging it. To put it rather crudely, the agenda to-date has been dominated by a no-win scenario:

2 The arguments presented in this chapter draw on sociological and policy research for two FP7-funded projects, Technolife, No: FP7-230381 (http://neicts.lancs.ac.uk/old/technolife.htm) and ICTethics, No: FP7-230368 (http://neicts.lancs.ac.uk/ictethics.htm). It is supported by two case studies within these projects, titled – *ICT for Human Security* and *Biometric Technologies* – but also on participation in expert meetings and workshops organised by the FP7-funded projects RISE, HIDE, and the BEST Network.

3 The Schengen agreement designates a border-less geographical area within Europe with border controls for travellers crossing the Schengen frontier borders but, ideally, not the internal borders.

4 US President Obama speaking to both houses of Parliament in the United Kingdom, 25 May 2011.

would 'you' not give up some civil liberties, personal data and privacy, so authorities can catch terrorists and keep you safe? This particular framing is not systematically challenged – of course you would – while it holds within the self-evidence of interoperable and integrated ICT systems, of biometric identification, visa registries and related applications (Amoore 2006). Ethicists and legal scholars have taken more or less at face value the focus here in governance on *striking the right balance* between the freedoms of individuals and providing them with security. Among other things, their work attempts to clarify what is at stake if a right to privacy and self-determination is diminished or taken away (see Laas-Mikko and Sutrop this volume). New privacy enhancing technologies have seen light, new data processing principles, and attempts are made to improve on existing legal frameworks in Europe, in particular, with the General Data Protection Regulation (GDPR) proposal (European Parliament 2013). However, this balancing metaphor does not adequately reflect citizens' perceptions which are found to be somewhat divided between those who see their privacy infringed on without improved security and those who see their security enhanced without privacy infringement (Pavone and Esposti 2010). More importantly, widely researched and debated concerns over first-world liberties and citizen rights, draw attention away from the role of the securitization agenda in protecting the free movement of data. Against concerns that rights and liberties are at risk and in need of protection from the very methods of delivering security, the free movement of data is the *versatile materiality* of economic competitiveness and growth. Productivity and cohesion depend on it along with the pursuits of other freedoms of movement with which transnational industries and markets progress.

Taking these considerations into account, the question remains how to re-frame the securitization agenda to foreground the issues that are obscured by the no-win scenario and the metaphor of striking a balance. Firstly, there is nothing to prove that authorities catch terrorists and criminals *because of* biometric registries and cutting-edge ICTs. There is nothing to suggest a categorical change in a long history of record-keeping and investigative techniques for operational and administrative purposes of states and constabularies. Advancing ICTs in surveillance and record-keeping, and implementing biometry for identification, is widely seen as a matter of efficiency, convenience and service quality (see Rommetveit, this volume). Secondly, when authorities identify threat and justify surveillance in the name of security, they appear to be targeting political activism against war and social injustices, including members of Occupy (Poitras 2014), or those who mobilize against various scientific, technological and other societal ventures (e.g. Welsh and Wynne 2013). In reference to *exceptional circumstance*, framed in militaristic terms as *threat* or as criminal investigation, authorities decide what they need and what to do, and involve publics by command, not consent and consultation (see Agamben 2005 on state of exception). In the United States, authorities are known to subpoena the online service industries and other commerce for the *personal* data they process, i.e., to gain insights into who the culprits are or these *publics-as-threat* on their watch lists. The result is a growing number of self-censoring publics, as we also learn from the Snowden revelations that authorities in European states have been depending upon access to precisely the same sorts of insights with assistance from the United States.[5] This *practical utility* of the securitization agenda has been shrouded in secrecy while the agenda is still *instrumental* in amplifying visions of vulnerable – but irrelevant – publics, apparently ignorant of the security threats surrounding them.

2 Mobilities: associations and relations

Transnational development in tourism, migration, markets and mobile employment are among the many study topics found in the academic discourse on contemporary mobilities. Mobilities research is focussed on the technological and material conditions of persons, objects and ideas on

5 See http://www.statewatch.org/eu-usa-data-surveillance.htm .

the move and in stasis. It aims to clarify the political, cultural and socio-economic relevance of mobility or the lack thereof (e.g. Gill et al. 2011; Scuzzarello and Kinnvall 2013; Jordan and Brown 2007; Stephenson 2006; Tyler 2006; Urry 2007). We learn how mobilities feature in personal, occupational and organizational lives, including the many "[i]ssues of movement, of too little movement or too much, or of the wrong sort or at the wrong time" (Sheller and Urry 2006: 208). Not only do persons and things flow through transits, but also through cyberspace by way of recordings and representations, and the re-creation of governance and prominent imaginaries using transportable media. In short, mobilities are deployed and consumed in the course of achieving what are considered normal commitments and obligations (Shove 2002). They satisfy a need to *sustain proximity* (Urry 2002), a *will to connection* (Sheller and Urry 2006), and they require constant management.

The EU/EEA and Schengen agreements are only two examples of a whole complex of relations and associations Europeans are committed to across the region, to align and mobilize common interests (Fig.1). The countries of Europe also enter into myriad of non-EU/EEA agreements. Consulting the EU Treaties Office Database reveals bilateral and multilateral treaties with USA, Canada, Brazil, China, and many other countries and regions around the globe. Among the shared interests are agriculture, commercial policy, competition, culture, economic and monetary affairs, education, energy, environment, fisheries, food safety, foreign and security policy, information society, research and innovation, taxation, trade and transport (see also European Commission, 2009).

These treaties represent economic, social and market opportunities, which has contributed to the

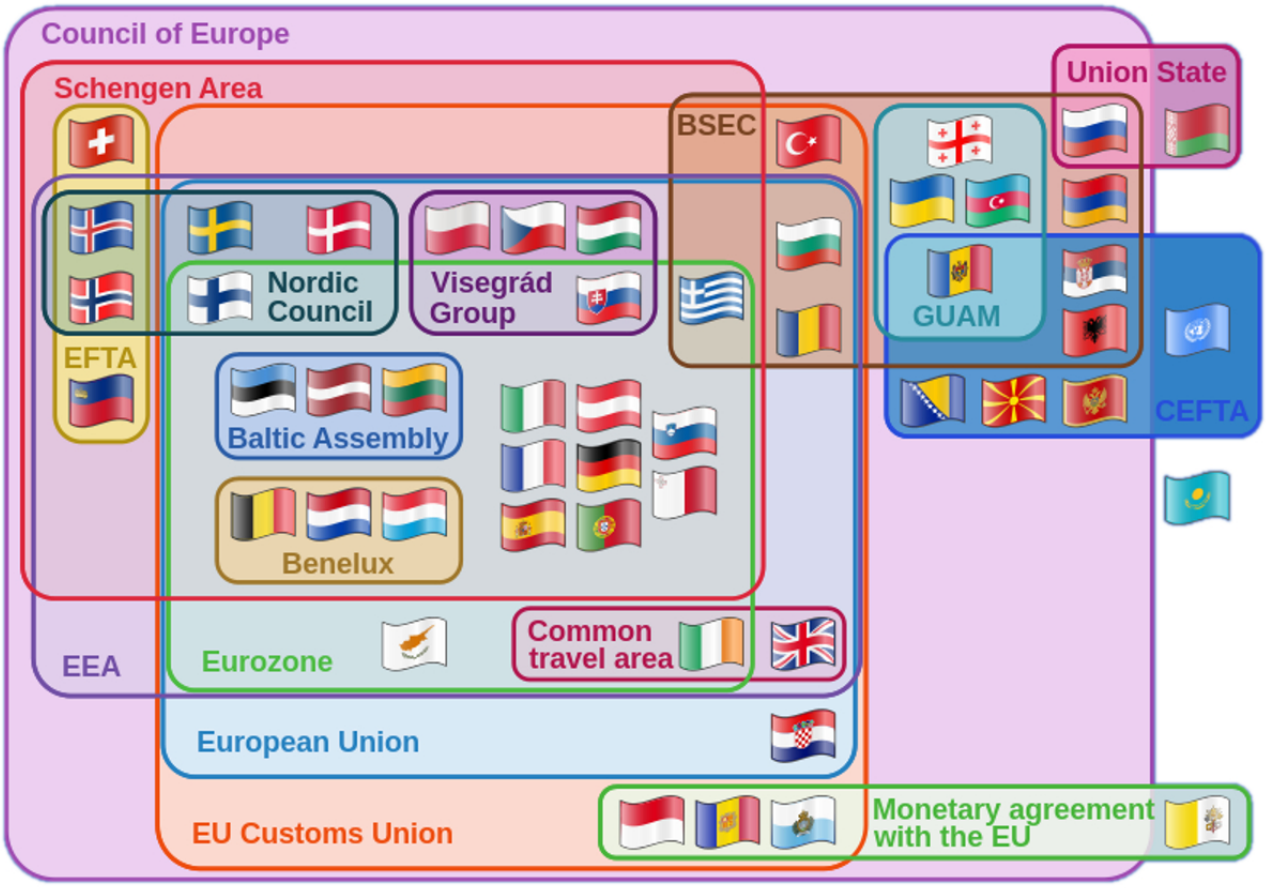

Fig 1: A diagram showing supranational relations and associations within the boundaries of the Council of Europe, plus Vatican City, Belarus, Kazakhstan and Kosovo. Associations across Europe change over time and so have the Euler diagrams in this and related Wikipedia entries, http://en.wikipedia.org/wiki/European_Economic_Area (May 2015).

normalization of mobilities as the way forward. On the face of it, these developments appear as "a promising sign of global newness and future-making" (Gill et al. 2011; Adey 2010), a form of cosmopolitanism, manifested in enhanced freedoms and opportunities to prosper across the globe in an era of declining nation states. However, we are warned against associating mobility uncritically with liberation from nationhood and widespread personal freedoms (e.g. Cresswell 2006). Borders and other checkpoints continue to delineate and connect, divide and categorize persons and cargo, reject, admit, contain and alienate, and they are contentious in political debate.

2.2 Politics of cohesion

The *instrumentality* of the securitization agenda is based in growing insecurities concerning economic, social and territorial cohesion. Across Europe, cohesion is seen as essential to the stability of the Single Market and the European Union (EU) has a pivotal role to play in staging its moral character on the basis of the EU constitution. The Union shall "offer its citizens an area of freedom, security and justice without internal frontiers, [...] combat social exclusion and discrimination, and [...] promote social justice and protection" as well as solidarity (European Union 2010, Art.3 of Common Provisions p.17). But, social and territorial cohesion is subject to doubt when the distribution of opportunities, wealth and welfare is unequal among member states, some of which are also grappling with internal unrest. States in Europe are not equal with respect to their governance traditions and development. There are significant differences to be observed between the northern, central and southern territories. Some states are richer than others and some more influential in cooperation on matters of economy, markets, innovation and societal affairs.

These differences influence the ways in which the mobility of persons is looked upon and managed. The current amount of mass irregular travel and nomadic labour was not anticipated in the early days of the Single Market and the entitlement to protection of labour conditions and mobility *for all* has not always been welcome, not even within Schengen. The second paragraph in Article 2 of the Schengen agreement allows for unilateral reintroduction of border checks, i.e., spot checks, which are periodically invoked in relation to events or *exceptional circumstance* seen as a threat to security and the public order (Council of the European Communities 2000; Apap and Carrera 2003). For example, migration anxieties surfaced in 2011, in relation to the so-called Arab spring when Italians saw an influx of migrants from the conflict zones on their shores (Scuzzarello and Kinnvall 2013). The decision to issue temporary residence permits to Tunisian refugees triggered patrol on the French-Italian borders to stop that migration going further north. Anti-immigrant sentiments were also heard in Denmark at the time, however, with focus not only on migrants from the Maghreb region, but from Poland and the Baltic states. Similar anxieties were evident in warnings of disproportionate migration resulting from the enlargement of the EU to eastern regions—concerns, not entirely void of scepticism about social-cultural kinship (Kvist 2004; Bauer and Zimmermann 1999). The delay in opening the doors to citizens of the new member states was allegedly to protect social infrastructures and, as these words are written, migration anxieties are soaring yet again in relation to a whole new refugee crisis, with huge numbers fleeing warfare in Syria over borders into Europe. Again, internal borders are being temporarily reinstated on a number of fronts and the outer Schengen borders reinforced.

Scuzzarello and Kinnvall argue that these kinds of events show how quickly borders are reclaimed and ideas of a collective self and national identity reinstated in political and media discourse. This happens periodically within the EEA and Schengen and one can argue that Europe remains geographically, culturally and economically divided regardless of the protection of freedoms to facilitate the Single Market and relations beyond.[6] Those from outside the EEA and the

6 Crossing patrolled borders between Norway and Denmark since the conflict with the Islamic State began, also illustrates some of the complications faced within Schengen when EEA citizens get involved in such conflicts.

Americas, in particular, from where asylum-seekers and economic migrants originate, are also neither wanted nor welcome by authorities. They are not the *ideal foreigners*, the educated and mostly white who arrive with social, cultural and economic capital to travel, study, work, consume and even settle (see Tyler 2006, on the UK case). There are opportunities *for some* to study and accept job offers across state lines and there is a tourist trade aimed at those with disposable incomes. Frequent long-distance travel remains privileged however, and so is effectively the so-called *global workforce*. As Castells puts it,

> [w]hile capital flows freely in the electronic circuits of global financial networks, labor is still highly constrained, and will be for the foreseeable future, by institutions, culture, borders, police, and xenophobia (Castells 2010: 247).

If these observations are anything to go by, only the privileged labour force of specialized professions are living their lives across national borders with relative ease and comfort (also Cooper and Rumford 2013). At the same time, an intensification of labour mobility and tourism was seen in all regions of the world toward the end of the last century (e.g. Massey et al. 1998) and the trend continues. Being *open for business* however, opens the doors to both legitimate and illegitimate flows. Mobile capital benefits from an authority structure that defends its mobility and privilege, but the intensification of dissidence and hostilities, aimed at free-market democracies and corporate enterprise, calls for new priorities in thinking about the cohesion of transnational markets. The securitization rationale has adopted narratives that depict particular kinds of flows as trusted against flows that are a threat to the socio-economic and moral order—narratives that mediate belonging, set the threshold for inclusion, and demand that mobility data is made available to authorities in the name of security.

3. Mobility controls and the *fifth freedom*

Drawing on mobilities research, one can argue that agreements like the EEA and Schengen constrain as much as they facilitate the freedoms of movement but, also, that the movement of data deserves closer attention. It is key to the *practical utility* of securitization. Modern states are increasingly more mobile to keep up with persons, capital and commodities (Beck 2005, 2008). They need to keep up with an economy which is *informational* as well as globally organized (Castells 2010), drawing together materials, commodities, markets and labour, along with the business models and the organizational management for which the free movement of data is an absolute necessity. Within the EEA, the free movement of data is effectively the *fifth freedom*, and even if not explicitly recognised as such, an *Informational EEA* is obliged to protect that freedom. This is evident, for instance, in the preamble of the GDPR, stating the aim to protect the free movement of data across the internal market.[7]

Historically, all sorts of data are processed for supervision and operational surveillance. For example, the types of surveillance on persons manifested in public registries have heritage in record-keeping and investigative techniques for social security entitlements, tax collection, election management, healthcare, border control, intelligence and ordinary policing. Outsourcing the processing of these data to private and corporate agencies has gone on for years, but the more advanced surveillance and security systems – including biometry – have a history as well in banking, industry, insurance and commerce (Lodge 2006).

A significant amount of data on persons is now in circulation throughout the economy (and

7 The title of the GDPR proposal also states that it is a "Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data" (in May 2015, the legislation of the GDPR in the EU Parliament was estimated to happen in 2017).

growing), either identifiable or clustered *by type* in reference to locality, mobility, biophysical profiles, action, preference, and behaviour.[8] Huge amounts of data on persons are processed by the service industries and in marketing with the bulk of it now generated by individuals themselves. Targeted marketing and so-called personalized services rely on customers volunteering data and, as the argument goes, blanket restrictions will harm competitiveness by undercutting existing business models, back-office efficiency, new service discovery and the delivery of customer service quality (European Parliament 2012).

It follows here that in a world in which mobilities are imperative to a successful trade across borders and regions, ICTs are essential to the surveillance of marketing efficiency as much as they are to the surveillance of productivity and returns. Research into targeted marketing has led the way for decades on how and why mobilities should be traced and monitored (e.g. Phillips and Curry 2003). For example, it has shown the difficulty in relating geographically localized populations (geodemographics) to sociological ideals about identity, lifestyle choice, circumstance and preference. These failings in defining localized groups suggests that knowledge of persons could be better established by following them around. Similar advantages are surfacing more recently with growing use of mobile sensors, i.e., to establish knowledge on movement, biophysical and health-related profiles. Transactions and logs are monitored to target any such knowledge with reasonable accuracy, for example, in using the internet, mobile and smart phones, sensors, service systems of sorts, machine-readable cards and any other transaction-type or logged event.

The analogy here with border control describes how any place, physical or virtual, can be turned into a *checkpoint*. Individuals are intercepted, asked to identify themselves and clarify their travels, activities and transactions, aspirations, intentions, the goods and keepsakes that travel in their name. These practices exemplify both facilitation and restriction of mobility, with private and corporate enterprise increasingly managing all manner of such checkpoints at their own discretion. The idea that people's intentions can likewise be detected and intercepted has gained significant momentum,[9] and the commercial interests and economic gains of the software and communications industries give rise to suspicion that governments are not entirely in control of how to regulate these developments. The *fifth freedom* here has neither been conspicuous nor transparent to publics at large. They are not critically involved in assessment and decision-making on matters concerning the collection and processing of personal and potentially sensitive data, nor the extent to which surveillance can be practised by private and corporate agencies for commercial purposes and economic gain.

3.1 Self-censoring publics

The securitization agenda has shifted the focus in law enforcement, security and related operations, toward pervasive surveillance for investigative purposes which takes advantage of the data flows in the service industries. As Lyon observed (2003), surveillance is “a feature of everyday life, at work, at home, at play, on the move” (p. 13), and the Snowden revelations provide stunning insights into precisely the extent to which surveillance takes place and how publics are targeted (Poitras 2014). The latest technological advancements are mobilized to this effect with the shift toward preventative scenarios involving research into the remote monitoring of persons in large numbers. Cameras are attached to video content analysis, combined with biometric techniques for

8 It can be argued that data clustering by types anonymizes data, i.e., the data controller is not interested any one person's official identity, only that such and such a person is of such and such a *type*. This is debatable however, since the goal is typically to be able to intercept *types of persons* via email, web browsing, phone messaging or old fashioned mail, all of which is ultimately traceable back to actual individuals.

9 See for example, https://www.informationsystems.foi.se/main.php/ADABTS_Final_Demo.pdf?fileitem=7340169 and http://en.wikipedia.org/wiki/Future_Attribute_Screening_Technology .

facial recognition, behavioural pattern recognition and remote sensing of physiological states. It is unclear however, what is actually achieved with all this data mining, statistical categorizations of *dangerous* groups, profiling of individuals, and ICT-assisted predictions of future events (on profiling see Hildebrandt and Gutwirth 2008; Hildebrandt 2008).

Serious doubts have been raised about the investigative and preventative scenarios in recent times, and it is yet unclear whether or not such systems eventually come online to achieve what designers have hoped for (Hornung et al. 2010; Schlanger 2011). Those who work within the agencies investing significant sums in this research are choosing their carefully, e.g., "it is not currently, and may never become, operational" or "deployment, if it ever occurs" (Schlanger 2011: 2). The technology does not appear to be very reliable and extensive ethical and legal reviews have called for adjustments, with some projects abandoned entirely or scaled down to small location-specific applications. As general investigative tools however, advanced surveillance systems along with the data logging and profiling that underpins existing business models, management and discovery in the service industries, are providing unprecedented access to data for search-and-match purposes.

The danger here is losing sight of opportunities to meaningfully object to the pursuit of executive powers to intercept data flows and logs in these systems. As Snowden has put it (Poitras 2014), publics are self-censoring if they live with the expectation of being watched all the time. Indeed, it appears that speaking of liberties and freedom has been captured in the notion of *privacy* in the very particular sense that *not having privacy* is a loss of a person's agency because they no longer feel free to express what they think (Applebaum, cf. Poitras 2014). Privacy is here primarily linked to freedom of speech and expression.[10]

> If we don't have our right to privacy, how do we have a free and open discussion? What good is the right to free speech if it isn't protected in the sense that you can't have a private discussion with somebody else about something you disagree with. Think about the chilling effect that that has. (Levison at the hearings in EU parliament on NSA surveillance of EU citizens and companies, Sept. 2013, cf. Poitras 2014, 1:38:45-1:39:05).

It may seem that a distinction between *private* and *public* needs to be ascertained here, and how the two intersect. Any given communication can be more or less private or public, and not obvious when indeed one is free to express one's opinion given the incentives to self-censor, for example, not to be associated with certain persons, politics and events, and not be put on some watch list or other. The same can be said about avoiding physical attire and behaviour that may give rise to alarm. But, distinctions of public and private are not at issue here, rather, the conditions by which self-censoring becomes a feature of everyday life. As it stands, individuals and groups are posed against a coalition of agencies, whose personnel are learning how the most advanced technologies can assist them in detection—how security and surveillance systems *aimed at everyone* can assist in establishing ever more detailed knowledge on *who they are* and if they are welcome or a threat, and in preventing certain kinds of events from happening. This positioning may well sit on a continuum with older investigative techniques used by state agencies and constabularies to put on a *display of power*, to uphold the rule of law, manage mobility risks and investigate acts of crime and terror. There are well known pros and cons concerning the application of ICTs and biometry as part of intelligence gathering, and such practices are continuously negotiated in reference to the rights and liberties of persons, what is proportionate, justified, and so on.[11] What is at issue here is rather the

10 Article 19 of the Universal Declaration of Human Rights (The United Nations 1948) states that everyone has the right to freedom of opinion and expression. However, widespread self-censorship is a well-known phenomenon, notably in recent US history during the McCarthy era and in recent European history east of the Iron Curtain.

11 An issue repeatedly foregrounded during the ICTethics expert workshop on "Human Security in the context of Ambient Intelligence", Nov 2010, Leeds, UK.

tensions that arise when such a versatile materiality of global economic competitiveness and growth, *data*, is exposed to exceptional circumstance, whereby personal data – in fact any data – can be subpoenaed or otherwise intercepted for purposes no one can truly challenge. The GDPR proposal, as it stands, may be an attempt to improve upon the protection of personal data, of clarifying the ramifications of data processing and retention in an era of increasingly more powerful technologies.[12] When it comes to pass however, it will have no force in challenging data operations relating to criminal investigations, security or terrorist prevention programmes—areas of activity where publics will need protection the most if the practical utility of securitization is primarily to target political resistance couched a as *threat to public safety and the socio-economic order*. Publics may have no choice left but to self-censor while there are still good reasons to speak up and act in defiance of authorities on a range of deeply contentious issues, including social injustices, decisions on warfare, the direction of the socio-economic system and the purposes more generally of scientific, technological and other societal ventures.

4. Keeping *what* safe? [13]

The four freedoms of movement, as stated in the EEA agreement, do not immediately signify how mobilities leave behind traces of transactions that open the doors to pervasive surveillance. It is not obvious either what the fifth freedom signifies in terms of how to protect individuals with regard to the processing of personal data. This chapter began by claiming that the securitization agenda emerges in consequence of *insecurities*, albeit, there is persistent lack of clarity on why securitization – as it proceeds – is made to seem inevitable. On the face of it, securitization has been justified in reference to enemies descending on first-world democracies and hiding *among* the citizenry. Indeed, the agenda has been particularly instrumental in cultivating migration anxieties, scepticism over entitlement to mobility and in framing a problem of *threat* in terms of an imperative to detect and identify those who are dangerous.

There is nothing to indicate here other than a continuity of familiar old-age problems of oppression and resistance, corruption, exploitation, abuse and terror, only that these problems appear in new guises and involve the latest technologies appropriated by enemies and allies alike. Narratives of threat and emergency mask this, along with a whole host of considerations that have a history of being ideological no-go zones. For example, openly debating with publics the very purpose and direction of first-world leadership in economic affairs, innovation and market competitiveness, might result in 'unpalatable' demands to do things differently. Such debates are yet to be had in organized ways and reported on in mainstream media, involving key decision-makers along with citizen juries or other recognised methods of public engagement.[14] Openly debating whether or not *our leadership* is sustainable, in particular, if it erodes the cohesion it is meant to aim for, may call for an honest reflection on the rhetoric of *leadership* and of *keeping us safe*. When used by leaders and mainstream media, such rhetoric draws the attention away from state-sponsored

12 As this is written (May 2015), legislating the GDPR is not expected to happen until 2017 after years already of preparations and thousands of amendments, many of which are watering down the obligations of data controllers in order to safeguard business models, economic and innovation competitiveness.

13 Some of these concluding remarks I owe to an inspiring meeting (Jan 2014) with the Icelandic parliamentarian, Birgitta Jónsdóttir and internet pioneer, Guðmundur Ragnar Guðmundsson, in particular, their thoughts on digital self-defence in contemporary consumer culture, and the lack of teeth in the GDPR proposal and similar efforts with respect to scope and jurisdiction.

14 Debates that really shake the core assumptions on which the economy rests, first-world leadership, innovation, security, etc., are held in small ways, involving whistleblowers, critics and disillusioned members of established institutions who find voice on minor media outlets, typically referred to as left wing or 'too' radical to be on par with mainstream communication, e.g., Democracynow! (http://democracynow.org), Counterpunch (http://www.counterpunch.org/) and New Statesman (http://www.newstatesman.com/).

aggression in defending vested interests across the globe, in goods, services, capital, mobile labour and *data* (also Herman and Chomsky 1988 on manufacturing consent). Furthermore, narratives of threat and emergency call for immediate intervention. Under the circumstances, government executives manipulate the legislature to rush through emergency laws, bypass the judiciary or ignore both, while going ahead with secret mass-surveillance programmes (Poitras 2014; Harding 2014).[15]

It is at this juncture that one can see that the insecurities in question here, centre to large extent on the *publics at home*. It is also at this juncture that the pivotal role of ICT-based innovation finds its relevance, as previously stated in this chapter, in conjunction with long-standing practical uses of surveillance and security technologies in industry, banking, trade, commerce and other service sectors. The intensity of contemporary surveillance has been more deeply political than fending off nebulous enemies from alien cultures who can harm us at any moment. Intelligence, observation and quantification techniques are used to code and classify persons according to definitions that are interpretatively flexible and ideal to identify those who mobilize against industry, finance, market and innovation policies, in the name of public safety (Welsh and Wynne 2013).

Even after the Snowden revelations began, little is yet done in the way of communicating and critically debating in the public domain the purposes with which intelligence and security operations proceed and, for Europe in particular, the limits in scope and jurisdiction of the GDPR (once legislated) in actually protecting persons. Given the strength of the official rhetoric of threat and emergency, and the silencing of opinion through self-censorship, this is not surprising. But, democratically elected bodies should be held to account for the ways in which ICT-driven surveillance operations are allowed to propagate as the inevitable way forward in defending *our way of life*. There is no evidence that advancing ICTs alone will help remedy dissent and hostility and cultivate cohesion. Rather, there is good evidence that the software and communications industries have significant investment in the securitization agenda, while the question remains to what extent the service industries and markets should comply with the agenda, given how much their investments depend on data-driven solutions (including targeted marketing).[16] In fact, they are faced with an impossibility. Authorities can very effectively leave most of the monitoring and measuring of everyday mobilities to private and corporate enterprise and issue subpoena when needed.[17] Technically, service providers can refrain from retaining data (metadata or content data), especially identifiable data, but authorities can still intercept all transactions under circumstances removed from democratic accountability. The only alternatives left then, are to close up shop or otherwise give way (Levison, cf. Poitras 2014, 1:37.02-1:38:20).

The persistent lack of clarity on the purposes of mass-surveillance, *what exactly is kept safe* and who is actually in charge, points to a need for open reflection and debate, albeit, public debates are not likely to lead if we have entered a climate of self-censorship and, to paraphrase Snowden, if the boundaries of intellectual exploration have been limited (26:54-26:58).[18] One could ask why publics at large are not more encouraged to consider the pre-eminence of their informational selves and

15 There are many attempts over the past decade to back-track on executive powers, e.g., in summer 2015, a disquiet in the UK parliament over the lack of transparency regarding the reach of executive powers, including the GCHQ, without the mandated checks and balances of a three-tiered government. The US Patriot Acts have also been revisited, the US surveillance law, the legality of the Guantánamo Bay detention camp, and more.

16 In the aftermath of the Snowden revelations, the big industry players in ICTs are publishing on this, e.g., IBM on regulatory affairs and Microsoft on public policy agendas, and there has been a gradual shift in recent years toward seeing privacy sensitivity as a resource for profitable innovation, e.g., in selling to prospective customers privacy-by-design and protection-by-design products and services.

17 Arrangements like that between government agencies and private enterprise are indicated in the Snowden revelations. Yahoo, Google, Facebook, YouTube and Skype were implicated in the PRISM programme (NSA) and the UK GCHQ accessing data on persons through that programme, thereby circumventing legal procedures.

digital citizenship.[19] As it stands, the majority of publics indulge the complacency which is part and parcel of free-market democracy—the comforts of consumption, of ready-to-hand products and services, leaving them vulnerable to marketeers and government agencies pushing uncontested agendas. The majority of publics may not see a risk to their mobility or to their "private and family life, home and communications" (European Communities 2007: Art. 7), and publics are not commonly educated in electronic and digital self defence. There are no provisions for such defence in the European or US constitutions,[20] but guarantees of interoperability between industry software and citizens' initiatives to build digital and informational safety around themselves are still a legitimate demand. As it stands, the software and communications industries cannot be obliged to use open-source encoding of software, say, of encryption algorithms, which means there are no adequate tools to keep industry software in check, in particular, for vulnerabilities to snooping and other illiberal practices.

What is publicly acceptable should be put to the test here against the practical utility of the securitization agenda, taking into account that public acceptability risks compromise when ill-defined threats encourage people to accept personal data gathering without asking what it is for (Pavone and Esposti 2010). The fifth freedom may certainly warrant protection for all sorts of practical, educational and entertainment purposes, however, as long as there are serious blunders in the checks on executive powers, the very idea of *having control* of personal data protection by way of law-making (the GDPR), or of one's privacy, is largely void of meaning. Having learned and enlightened debates across the Atlantic on the importance of privacy, liberty and self-determination in the making of first-world democracies, on striking the right balance, and so on, is equally futile when any data that can be collected is, in all likelihood, collected eventually by some agency, overtly or covertly, processed, disseminated and retained for purposes that are obscured from view and cannot be contested. These topics have yet to enter into dialogue that can exercise legitimate powers of participation and persuasion—to engender a critical re-framing and re-evaluation of the securitization agenda with a view to much greater checks on executive powers along with a debate and deliberation on the kinds of future societies first-world citizens can imagine for themselves, not just at home but in relation to the rest of the world.

References

Adey, Peter. 2010. *Mobility*. London: Routledge.

Amoore, Louise. 2006. Biometric borders: Governing mobilities in the war on terror. *Political Geography* 25(3):336-351.

Agamben, G. (2005). *State of Exception*. University of Chicago Press.

Apap, Joanna and Sergio Carrera. 2003. Maintaining Security within Borders: Towards a Permanent State of Emergency in the EU? CEPS Policy Briefs 41, October 2003. [Policy Paper].

Bauer, Thomas and Klaus F. Zimmermann. 1999. Assessment of possible migration pressure and its labour market impact following EU enlargement to central and Eastern Europe – A Study for

18 See also interview with Glenn Greenwald and Laura Poitras (9 June 2013), in which Snowden elaborates one of his key arguments that publics need to be consulted and somehow involved in decisions on the extent to which personal data handling is publicly acceptable, in particular, in light of the self-censoring going on. Available at http://www.theguardian.com/world/video/2013/jun/09/nsa-whistleblower-edward-snowden-interview-video (visited Feb 2014)

19 For example, there could be widespread education programmes from primary school level and upward, teaching on these topics, both practice and theory.

20 It is of some curiosity that US citizens have a constitutional right to armed defence of their person and property against threat and oppression, but no such right to defence of their informational person and property.

the Department for Education and Employment, United Kingdom. IZA Research Report No. 3. http://www.iza.org/en/webcontent/publications/reports/report_pdfs/report_pdfs/iza_report_03.pdf. Accessed Jan 2014.

Beck, Ulrich. 2005. *Power in the Global Age: A New Global Political Economy*. London: Polity.

Beck, Ulrich. 2008. Mobility and the cosmopolitan perspective. In *Tracing Mobilities. Towards a Cosmopolitan Perspective*, eds. Weert Canzler, Vincent Kaufmann, and Sven Kesselring, 25-36. London: Ashgate.

Bigo, Didier. 2007. Mobility Controls and New Technologies. In *Are you who you say you are? the EU and Biometric Borders*, ed. Juliet Lodge, 9-14. The Netherlands: Wolf Legal Publishers (WLP).

Carothers, Thomas. 2003. Promoting Democracy and Fighting Terror. *Foreign Affairs*, January/February. http://www.foreignaffairs.com/articles/58621/thomas-carothers/promoting-democracy-and-fighting-terror. Accessed Jan 2014.

Castells, Manuel. 2010. *The Rise of The Network Society. The Information Age, Economy, Society and Culture, Volume 1 (2nd edition with a new preface)*. Wiley-Blackwell.

Cooper, Anthony and Chris Rumford. 2013. Monumentalising the Border: Bordering Through Connectivity. *Mobilities* 8(1): 107-124.

Council of the European Communities. 2000. The Schengen Acquis. Official Journal L 239, 22.9.2000. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:239:0001:0473:EN:PDF. Accessed Jan 2014.

Cresswell, Timothy. 2006. *On the Move: Mobility in the Modern Western World*. Taylor & Francis.

Dalacoura, Katerina. 2005. US democracy promotion in the Arab Middle East since 11 September 2001: a critique. *International Affairs* 81(5): 963-979.

European Commission. 2009. External Relations. European Community/European Union. http://eeas.europa.eu/association/docs/agreements_en.pdf. Accessed Jan 2014.

European Commission. 2008. Data Protection in the European Union – Citizen's perceptions (Flash Eurobarometer 225), Feb.2008. http://ec.europa.eu/public_opinion/flash/fl_225_en.pdf. Accessed Jan 2014.

European Communities. 2007. Charter of Fundamental Rights of the European Union. Official Journal C 303/01. http://eur-lex.europa.eu/en/treaties/dat/32007X1214/htm/C2007303EN.01000101.htm. Accessed Jan 2014.

European Parliament. 2012. Data Protection Review: Impact on EU Innovation and Competitiveness (Study). Directorate General for Internal Policy. Policy Department A: Economic and Scientific Policy. PE 492.463. http://www.europarl.europa.eu/RegData/etudes/etudes/join/2012/492463/IPOL-ITRE_ET(2012)492463_EN.pdf .

European Parliament and the Council of the European Union. 2013. Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Unofficial consolidated version after LIBE Committee vote; Provided by the rapporteur, 22 Oct. 2013. http://www.janalbrecht.eu/fileadmin/material/Dokumente/DPR-Regulation-inofficial-consolidated-LIBE.pdf. Accessed Feb 2014.

European Parliament Fact Sheets. 2000. 6.3.2. The European Economic Area (EEA). European Parliament. http://www.europarl.europa.eu/factsheets/6_3_2_en.htm. Accessed Jan 2014.

European Union. 2010. Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union & Charter of Fundamental Rights of the European Union. Official Journal C 83, 30.3.2010. http://eur-lex.europa.eu/JOHtml.do?uri=OJ:C:2010:083:SOM:EN:HTML. Accessed Jan 2014.

Gill, Nick, Javier Caletríob, and Victoria Mason. 2011. Introduction: Mobilities and Forced Migration. *Mobilities* 6(3): 301-316.

Harding, Luke. 2014. *Snowden Files*. UK: Guardian Books.

Herman, Edward S. and Noam Chomsky. 1988. *Manufacturing consent: the political economy of the mass media*. Pantheon Books.

Hildebrandt, Mireille. 2008. Profiling and the rule of law. *Identity in the Information Society* 1:55-70.

Hildebrandt, Mireille and Serge Gutwirth, eds. 2008. *Profiling the European citizen: cross-disciplinary perspectives*. Dordrecht, NL: Springer.

Hoback, Cullen, director. 2013. *Terms and Conditions May Apply*. USA: Hyrax Films.

Hornung, Gerrit, Monika Desoi, and Matthias Pocs. 2010. Biometric Systems in Future Preventive Scenarios - Legal Issues and Challenges. In *Proceedings of the Special Interest Group on Biometrics and Electronic Signatures (BIOSIG 2010) Darmstadt, Germany 9-10 September 2010*, eds. A. Brömme, and C. Busch, pp. 83-95. Gesellschaft für Informatik e.V. (GI).

Jordan, Bill and Philip Brown. 2007. Migration and Work in the United Kingdom: Mobility and the Social Order. *Mobilities* 2(2): 255-276.

Kvist, Jon. 2004. Does EU Enlargement Start a Race to the Bottom? Strategic Interaction among EU Member States in Social Policy. *Journal of European Social Policy* 14(3):301-318.

Lodge, Juliet. 2006. Communicating (in)Security: A failure of Public Diplomacy. CHALLENGE: Research Paper no.3. Centre for European Policy Studies, Brussels. http://www.libertysecurity.org/article1155.html. Accessed Jan 2014.

Lyon, David, ed. 2003. *Surveillance as Social Sorting: Privacy, risk, and digital discrimination*. Routledge.

Massey, Douglas, Joaquín Arango, Graeme Hugo, Ali Kouaouci, Adela Pellegrino, and J. Edward Taylor. 1998. *Worlds in Motion: International Migration at the End of the Millennium*. Oxford University Press.

Meltzer, Joshua P. 2014. *The importance of the internet and transatlantic data flows for U.S. and EU trade and investment (working paper 79)*. The Brookings Institution: Global Economy & Development Program.

Obama, Barak H. 2011. President Obama Addresses the British Parliament, Westminster Hall, 25.5.2011 London, United Kingdom. http://news.bbc.co.uk/democracylive/hi/house_of_commons/newsid_9495000/9495513.stm . Accessed Jan 2014.

Pavone, Vincenzo and Sara D. Esposti. 2010. Public assessment of new surveillance-oriented security technologies: beyond the trade-off between privacy and security, *Public Understanding of Science* 21(5), 556-572.

Phillips, David and Michael Curry. 2003. Privacy and the phenetic urge: geodemographics and the changing spatiality of the local practice. In *Surveillance as Social Sorting: Privacy, risk, and digital discrimination*, ed. David Lyon, 137-152. Routledge.

Poitras, Laura, director. 2014. *Citizenfour (documentary)*. Praxis Films in association with Participant Media and HBO Documentary Films; in co-production with Bertha Foundation,

Britdoc Circle, Channel 4, NDR and BR Media.

Schlanger, Margo, reviewing official. 2011. Civil Rights/Civil Liberties Impact Assessment. Future Attribute Screening Technology (FAST) – Interactive and Passive Programs. USA Department of Homeland Security. http://www.dhs.gov/xlibrary/assets/crcl/crcl-assessment-fast.pdf. Accessed Feb 2014.

Scuzzarello, Sarah and Catarina Kinnvall. 2013. Rebordering France and Denmark. Narratives and Practices of Border-Construction in Two European Countries. *Mobilities* 8(1): 90-106.

Sheller, Mimi and John Urry. 2006. The new mobilities paradigm. *Environment and Planning A* 38(2): 207-226.

Shove, Elizabeth. 2002. Rushing around: coordination, mobility and inequality. Draft paper for the Mobile Network meeting, Oct. 2002, Department for Transport, London. http://www.lancaster.ac.uk/staff/shove/choreography/rushingaround.pdf. Accessed Jan 2014.

Stephenson, Marcus L. 2006. Travel and the 'Freedom of Movement': Racialised Encounters and Experiences Amongst Ethnic Minority Tourists in the EU. *Mobilities* 1(2): 285-306.

The United Nations. 1948. The Universal Declaration of Human Rights, UN Publications. http://www.un.org/en/documents/udhr/ . Accessed Jan 2014.

Tyler, Imogen. 2006. 'Welcome to Britain': the cultural politics of asylum. *European Journal of Culture Studies* 9(2) 185-202.

Urry, John. 2007. *Mobilities*. Polity Press.

Urry, John. 2002. Mobility and Proximity. *Sociology* 36(2): 255-274.

Welsh, Ian and Brian Wynne, B. 2013. Science, Scientism and Imaginaries of Publics in the UK: Passive Objects, Incipient Threats. *Science as Culture* 22(4): 540-566.