SURVEILLANCE LEGISLATION IN NORTHERN EUROPE: WHO WILL BE MY PRIVACY'S KEEPER?

Burkhard Schafer

Professor of Computational Legal Theory, The University of Edinburgh, School of Law
SCRIPT Centre for IT and IP law
Old College, Edinburgh EH8 9YL, UK
b.schafer@ed.ac.uk

Keywords: ***Online surveillance, comparative law, human rights***

Abstract: *This paper reports some initial findings of the Nordforsk funded «Eyes Online» project that aims to elicit how the legal systems of the UK, Norway, Sweden and Finland have reacted to advances in surveillance technologies and capabilities. Focus of the analysis is the concept of «border», not just as a demarcation between jurisdictions or nations, but as an ordering principle of the law that can be challenged, transformed and subverted through technology.*

1. Introduction

The paper discusses research carried out as part of a Nordforsk-funded project – «Taking Surveillance Apart: Accountability and Legitimacy of Internet Surveillance and Expanded Investigatory Powers», that brings together partners from police and academia in the UK, Finland, Sweden and Norway.[1] By combining expertise from criminology, human geography, law and computer science, the aim of the project is to analyse how the recent wave of surveillance legislation responds on the one hand to technological changes, on the other to public disquiet about ever increasing state powers. The project aims to conceptualise and understand these developments through the theoretical lens of «borders». This does not just mean physical or jurisdictional borders. Rather, we use a broader concept that also includes borders between disciplines, between social roles and functions, or conceptual borders between normative and descriptive discourses. The overarching question is if an increased misalignment between the way in which citizens and civil society, law and law enforcement, and the technology community frame each make sense of online activities leads to a loss in accountability and legitimacy of police investigatory actions. The second question is if European human rights law is an effective tool to mitigate these tensions, capable of shaping a surveillance regime that is on the one hand gives the state necessary police powers, while at the same time holding those wielding these powers accountable in such a way that public legitimacy of these powers as preserved. The alternative could be that changes in surveillance capabilities, the way the law conceptualises them and the way they are used in actual investigatory practice have created systematic gaps in the protective net of human rights law that raises question of legitimacy and democratic control. Even though abstractly, the recognition of human rights found its expression in international and supranational legal instruments, for most practical purposes the main guarantor of these rights remained connected to the concept of the nation state, with governance structures that focus on the protection of citizens (and, potentially to a lesser degree already, resident aliens) against abuse of power by their government. Both legal (judicial review; procedural exclusionary rules etc) and political (right to petition etc) governance mechanisms continue to reflect this approach. Correspondingly, in the political discourse surrounding surveillance powers, both in Europe and the US, frequent distinctions are made between (presumably unproblematic) monitoring of foreigners and the much more sensitive monitoring of citizens. However, given

[1] https://sites.dundee.ac.uk/eyes-online-project/about-the-project/.

the increasing integration of police activities, in Europe e.g. promoted through the recent and the increasing mobility of digital devices, this separation increasingly fails to capture the social reality of technology use.

A typical example of this new wave of legislative instruments is the recently enacted Investigatory Powers Act (IPA) in the UK. The Investigatory Powers Act 2017 expanded existing communications data retention requirements and created new powers for law enforcement agencies to intercept and collect communications data – including data from sources outside UK territory. It also created the legal basis for untargeted bulk collection of data, and a new supervisor regime to ensure that these significant new[2] powers are not abused.

In Finland the Coercive Measures Act 2014[3] has aimed at extending and updating key investigatory powers to meet the demands of the digital age. Meanwhile, the government launched two parallel legislative projects in 2015 to update the statutory foundation of military and civilian intelligence activities, including the surveillance of data networks and digital communications. While the official policy of the Finnish Ministry authorities claims that the intention is not to establish mass surveillance, the proposition to change legislation for collecting intelligence on communications data inside Finland's borders without reference to a specific crime has faced criticism. Currently communications data interception may be directed only at a message that originates from or is intended for a suspect in an offence (Coercive Measures Act: Chapter 10 Section 3) and online mass surveillance is thus not allowed. Exemplifying the type of political discussion that underpins these types of proposals is in Finland the position of the technology industry, that emerged as the strongest critic of these proposals, a role previously held by civil society groups. Several industry voices argue that the benefits of mass surveillance for maintaining security and detecting crime are lower than the costs of collecting and storing data as well as the cost of damaging Finland's reputation as a safe place for computer security business.

In Norway, the EU Data Retention Directive, enacted in 2006, was transposed into Norwegian law in 2011, and should have been implemented in spring 2012. Implementation however was postponed several times due to the criticism from the Norwegian Data Protection Authority, civil rights campaigners, data protection activists and lawyers. After the Court of Justice of the European Union declared the Directive invalid in 2014, the government put the directive on hold until the proposal is refined. There are still plans to give authorities wider powers to monitor information networks and to gather mass communications data. A new Security Act has been drafted, and there have been proposals by Intelligence Service to introduce digital border surveillance, and by the Norwegian Police Security Service to register conversations on social media and to analyse information from open channels.

While there is therefore a general desire by governments across the three jurisdictions to update surveillance legislation in response to both perceived new threat scenarios and an increased technological capacity to intercept and analyse vast quantities of data, there remain significant differences in the way in which public discussions about increased surveillance powers play out, whose voices are heard and listened to in these debates, and how far governments can go (and indeed how far police and law enforcement actually wants them to go) in enacting new surveillance legislation. To stay briefly with the last example, Norway delayed implementation of the Data Retention Directive and eventually abandoned the project when the European Court of Justice voided the underlying Directive. The UK by contrast implemented the Directive straight away, with the first part in place as early as October 2007, and the remainder transposed into UK law through the Data Retention (EC Direction) Act of 2009. When the ECJ declared the underlying Directive in violation of EU Human rights law, the UK did not withdraw these laws, but by enacting the Data Retention and Investigatory Powers Act (DRIPA) in July 2014 created a new, now entirely domestic legal basis for the police and security services to retain their existing powers to access telephone and Internet records, and concomitant storage

[2] It is contested just how new some of these powers are, the British government arguing that they mostly only clarify already existing powers, a view not universally shared by academic commentators, see Schafer 2016 for further references.

[3] An English translation is at http://www.finlex.fi/en/laki/kaannokset/2011/en20110806_20131146.pdf.

duties. Controversially, the Act also made it clear[4] that these requirements also apply to foreign companies, based abroad, whose telephone and Internet services are used in the UK. DRIPA was challenged in domestic and EU courts, and in July 2015, the High Court issued an order that parts of the Act were unlawful, and to be disapplied until 31 March 2016. We can see in this example not only considerable differences in the role and impact that civil society, national Data Protection authorities and data protection activists with expert knowledge have in influencing the legislative process, we also see different roles for the courts in responding to governmental overreach, with the UK government frequently testing the limits of what is permissible, only to react with marginal adjustments when the courts eventually declare the proposal as unlawful.

Explaining this divergence of approaches to surveillance legislation and the interpretation and implementation of EU and ECHR law between countries that otherwise show considerable similarity in their social, political and economic make-up and which are (for the time being at least) either EU member states or, in the case of Norway, partner in several EU law enforcement projects and closely following applicable EU law, is one of the aims of this project. That UK privacy law has often been misaligned with that of continental Europe is not a new insight. As a member of the common law legal family, its privacy law followed a somewhat different trajectory from that of the civilian systems of continental Europe. The common law never developed a self-standing doctrine of privacy torts, a position reaffirmed in *Wainwright v Home Office*[5], and addressed issues of privacy invasion instead through the doctrine of breach of confidentiality[6]. By contrast, jurists such as Otto von Gierke developed in civil law jurisdiction in the 19th century the notion of a general personality right, which would also eventually form the foundation for a self-standing privacy tort.[7] This general personality right was in Germany finally codified in the post-war constitution. Using the Nordic countries with their own distinct legal «mentality» as a comparator can help to elucidate further the role of these different legal mentalities or mode of problem solving in the way in which countries implement legal regimes that within Europe are meant to be uniform, but in concrete practice can still differ significantly.[8]

Second, apart from this system-internal dynamics that lead to a divergence between common law, civilian and, possibly, Nordic jurisdictions, differences between historical experience with oppressive regimes are sometimes given as a reason for the post-war divergence between the UK approach to surveillance regimes and that of continental Europe. While discussion in continental Europe have been shaped by the experience of living under totalitarian regimes, from Nazi Germany to the communist regimes in eastern Europe, the UK has never experienced, or at least prides itself as never having experienced, a massive and systematic abuse of surveillance powers by an authoritarian regime against its own population. As a result, public support for surveillance methods by the police is higher in the UK. But if this explanation is correct, we should find relevant convergences between Norway, Sweden and the UK, with Finland, having had a difficult and ambiguous existence in the shadow of the Soviet Union, as an interesting third comparator. Our approach therefore also hopes to elicit the plausibility of these common tropes in explaining divergence between surveillance legislation.

Finally, the study with its focus on the concept of «border» is particularly timely in the light of recent events. The Snowden revelations did not just show the extend of state surveillance, it also showed how national legal controls had been circumvented through international data sharing and collaboration between security services. This again was particularly true for the UK and its historically strong links with the US. This issue received additional poignancy through the decision of the UK to leave the EU and the jurisdiction of the European Court of Justice. In future data sharing and data transfer agreements between the EU and the UK, a finding of

4 This too has been subject to discussion. The government maintained that issuing of extraterritorial warrants was already possible under the 2000 Regulation of Investigatory Powers Act, a view opposed by most academic commentators, see Rauhofer/Abel/Brown 2014.

5 Wainwright v Home Office [2003] UKHL 53.

6 Richards/Solove 2007.

7 Götting/Schertz/Seitz, Handbuch des Persönlichkeitsrechts, § 2, Rn. 14.

8 See e.g. Legrand 1996 and Linarelli 2002.

«adequacy» of the UK data protection regime will be necessary, something that at the very least can't be taken for granted.

In Norway and Finland by contrast, as we saw above, publicly contested legislative reform is in process, so the issue which direction surveillance regimes across Europe are taking, and to what extend they respond to public disquiet, is particularly pertinent. Questions to be addressed in this context are if there is a distinctive European consensus emerging, or maintained, vis a vis the US dominance of Internet technology and the resulting surveillance capabilities, or are there fissions emerging? And if so, are these in line with changing public perceptions, or is there a widening gap between legislative and technological surveillance capabilities and public acceptance, not just by privacy advocates and activists, but society at large? If so, are there legitimacy gaps emerging that require different types of legislative response – and in particular, a greater emphasis of cross-border protection of human rights and privacy as opposed to merely national supervisory agencies, which may also be restricted in their focus on the rights of nationals, leaving an increasingly mobile global work force in a precarious state? To illustrate this last point, the new UK data protection regime explicitly creates an exemption for data collected for immigration administration purposes, leaving among others 3m European citizens in the UK who are undergoing the post-Brexit registration process with more limited protection. A legal challenge by the Open Rights Group and the 3 Million group on behalf of EU immigrants has been given leave at the High Court to challenge schedule 2, part 1, paragraph 4 of the new Data Protection Act which removes some data rights if that data is processed for the «maintenance of effective immigration control». This includes the right to access data, to restrict processing, to object to processing and the right to erasure, all provided for in the GDPR. This type of «two-tier system» of data protection rights, brings the issue of borders (geographic and conceptual) into sharp focus, and reminds us of the dangers of emerging protective gaps in our human rights regime.

The project combines doctrinal legal analysis with mainly socio-legal and criminological research methodologies. As we just saw, divergent developments in surveillance regimes can be attributed to law-internal, largely doctrinal differences, but also much wider culturally mediated differences in attitudes to surveillance, state power, and how and where «borders» of legal protection are drawn, something akin to Legrand's «legal mentalities». In the next section we describe some of the groundwork that we carried out to lay the foundation for such a multi-methodological analysis.

2. Comparative surveillance law

2.1. Methodological considerations

In the first part of the project, we map out some of the ways in which the current (and proposed) surveillance laws in the three countries draw various borders – between legal and illegal, protected citizen and unprotected foreigner, police and private sector. The starting point is a comparative functional analysis in the tradition of Zweigert and Koetz[9], as operationalised by Schlesinger[10] in the common core project, but with a focus on the differences between legal systems, taking convergence as the «null hypothesis» due to the shared European legal framework. Schlesinger proposed as methodology a – a four-step process. Step one consists in setting out a working paper with questions and hypotheticals, that was circulated among the project partners. The hypotheticals are the «real life» problems suggested by Zweigert and Koetz as the «tertio comparationis», and should be formulated ideally in a way that does not rely on legal vocabulary or legal conceptualisations that are specific to any of the systems studied. In step two, legal experts for each system wrote an individual report

[9] Zweigert/Koetz 1996 chap 1.

[10] Schlesinger 1957.

answering the specific questions by applying his law.[11] Step three was a discussion of the individual reports during project meetings. In the Schlesinger methodology, step four would have consisted of drafting a general report ,which would be unanimously agreed upon, that pointed out differences and commonalities of the legal systems that were subject to the study.

At this point we deviate from the Schlesinger model in two ways. First, we do not yet compete the doctrinal analysis – rather, in a reiterative process new hypotheticals and variants will be created in response to the answers by the national experts to the first set of questions. This is necessary as the answers showed that the scenarios for some jurisdictions, but not others, under-specified the question. This can be due to a number of reason, not all directly the result of differences in the applicable law. This can be further teased out through more refined scenarios.

Second, we treat the functionalist analysis as a mere stepping stone, but ultimately only an initial step to answer the question of the legitimacy of new surveillance powers. It helps us to formulate more precise research questions that can then be addressed through a socio-legal perspective, that correlates the abstract doctrinal analysis with empirical research into on the one hand public perceptions of surveillance and its impact on everyday behaviour, on the other a qualitative analysis of the stakeholder opinions on surveillance capabilities. For the former, we will conduct a series of questionnaire based interviews that will aim to establish how aware Internet users are – and to what extend their online behaviour is influenced by – the legal framework surrounding surveillance in their country. For the stakeholder analysis, we will in this part of the study we explore stakeholders «views on law enforcement and intelligence agencies» online surveillance capabilities to monitor online communications and behaviour. The stakeholder groups we interview for this study are for example public authorities, politicians, private companies, non-governmental organisations, media representatives and researchers. Participants are selected based on their opinion on online surveillance: we try to cover as many different views as possible. About 30 interviews will be made in Finland, Norway and the UK between the summer and autumn 2018, using q-methodology to identify patterns within and between jurisdictions. The findings of these two studies will then be re-connected to the doctrinal comparative analysis. By combining a functionalist comparative analysis in a novel way with empirical research into public attitudes, the hope is to establish a much more fine grained analysis than usually possible how specific legal approaches and doctrinal constructions are reflective of path-dependent legal doctrinal factors, responses to public perception, or best explained by political processes and power differentials. The next section of the paper reports some of the findings of the first stage of this reiterative process.

2.2. Hypotheticals

We designed five case studies or hypotheticals, each designed to elicit some of the «border issues» that our theoretical framework focusses on. A total of 33 questions introduce additional variations and direct the attention of the legal experts to the theoretical issues the scenarios aim to elucidate. Once the process is completed, we will make all reports and the scenarios available through the project website. For time constraints, we introduce here only the «top level» scenario and its context – each of them has been the basisfor further variations and follow ups.

Case 1: The police has received some credible evidence that Mr T, a citizen within their jurisdiction, is involved in money laundering for organised crime groups. To find out more about his contacts, the police wants to plant a Trojan on his laptop. They request the help of a government agency that hosts a website he frequently uses for e-government purposes (e.g. an online tax form or vehicle registration agency) to install malware on Mr T's laptop when he visits their site. After the next start of his laptop, this software records all his browsing history

[11] The Finnish rapporteur was Johan Boucht, the Norwegian rapporteur was Ingvild Bruce, both from the University of Oslo, the UK report was compiled by Andrew Agnew. Their excellent work was a major contribution to the project, any misunderstandings and mistakes in this paper are the author'.

and the addresses and content of his emails. After a few days, Mr T travels with his laptop to a neighbouring EU country. The Trojan keeps sending information about his browsing behaviour from his new destination back to your police. A few days later still, he leaves the territory of the EU and travels to the US. His laptop stays with him there too.

Case 2: The police aims to improve its responses to human trafficking and sex slavery. To get a better picture of the evolving threat, and to identify potentially vulnerable children who could be potential victims, they want to combine their own information with data from schools, hospitals, social services, and also data from social media. They present at an internal briefing two use cases:

A) For domestic child grooming investigations, they want to correlate information from social services, schools, police and hospitals with social media data. Machine learning algorithms will identify correlations between risk profiles developed in multi-agency contexts and the social media presence of the children so identified. The aim is to use the analysis of social media posts to identify children at risk, and to understand better the linguistic cues they leave behind in their posts, e.g. when they talk about being befriended by older males or asked to do inappropriate things in video chats. The project has 2 aims: First, to find patterns in online behaviour that should raise red flags, to assist in the future parents, teachers or social workers in spotting early warning signs. Second, and more ambitiously, the want to use the algorithm to automatically identify children at risk and direct support resources specifically at them. The police emphasise that this is not meant punitively, or in preparation of prosecutions, but merely preventative and assistive.

B) For sex trafficking from overseas, the same algorithms are to be used to analyse social media abroad for indications of being lured into sex slavery or similarly exploitative schemes. As an example, correlation between geo-location data and police intelligence would identify villages in Russia as a common source of trafficked woman, analysis of correlated Facebook sites would then allow to identify potential victims (e.g. posts of the form «v. excited to have been given an au pair job in XYZ! Will travel soon, everything arranged by X» (where X may or may not have been on the police radar).This will then allow to intercept the traffickers upon arrival in your country before their victims come to harm

This case covers algorithmic decision making and the border between human/machine intelligence. It introduces non-specific, suspicion free surveillance and data analysis. It also has an obvious geographical dimension. Finally, it addresses the border between victim and criminal (the victims of trafficking in the 2. Scenario will also be illegal immigrants for immigration law purpose. Finally, the variation introduces the difference between physical and virtual spaces.)

Case 3: A criminal group sells child pornography from a website on the Silk Road, the «bazaar» of the Darkweb. Payment is in bitcoins, and in order to get access to the most harmful material, potential buyers must first share some of their own illegal content to show their «bona fide» and tip their hands. A group of «white hat» hackers, or «online vigilantes» spoof that website, populate it with some realistic, but in reality computer generated images of nude children. They hope to attract potential buyers so that they can insert code into these images that allows tracking them, rendering the anonymization tools they have been using and the bitcoin encryption mood. They then pass on this information to the police.

This case is about the border between citizen and police, surveillance and sousveillance. It is also about «places» or «spaces» not yet often discussed, with obvious topical relevance, such as darknet and bitcoin.

Case 4: A criminal organisation infects computers that visit a website hosted by them with ransomware. To regain control of their computer, victims have to make a bitcoin transaction to a specific account, and also send the link on to at least 3 other people who they know will get infected in the same way. Victims come from all over the globe. The website is hosted on a server in the US, the recipient of the bitcoin transaction according to police intelligence in Russia. Your country is badly affected by the attach – the Ponzi scheme that it uses has resulted in the infection not just of thousands of private computers, but also of critical system such as hospitals and medical doctors, airlines ,supermarkets and food distributors, and some police forces. To stop the spread

of the infection, the police wants the identities of everybody who visited the website. Mrs T is a victim of the crime and living as citizen in your jurisdiction. She has sent the link as requested to two acquaintances living in other parts of your country, one to an address abroad. She has not paid yet but is about to.

Case 5: The national parliament has become target of a co-ordinated cyberattack. The emails of several parliamentarians, including those of cabinet ministers, have been compromised. Initial computer forensic investigations have indicated that the likely source for the attack came from abroad, the country of Borduria. A hitherto unknown group, styling themselves as «Bordurian Freedom fighters», claims responsibility for the attack. However, the sophistication of the attack indicates that it is likely that the attackwas either state sponsored, or at least carried out by groups with very close links to the Bordurian government. The relation between your countries have been strained, and Borduria is known to have used its extensive IT capacities to interfere with its neighbours IT systems before. However, it can also not be ruled out that the attack originates from your country, or has anything but mere commercial motives (blackmail, or selling compromising secrets to newspapers). One of the potentially compromising secrets that the attack may have leaked is «Operation cashback» –the illegal but government sanctioned payment of bribes to a foreign official of Khemed to facilitate the sale of «Seahawk» missiles that your country has developed. If this information became public, this would harm your countries international relations and reputation, and also cause significant economic damage as foreign sanctions against your arms industry are likely. To mitigate the risk, and identify if possible the perpetrators, your relevant agencies plan to

- Monitor all email traffic from your country to Borudia that contains the words «Seahwawk», «cashback» and «missiles» and «Khemed» –knowing in advance that the majority of these will be innocent exchanges
- Monitor email traffic between addresses in Borudia, for these words –asking for the help of allied countries that may host servers through which these emails are exchanged.
- Ask these countries to share communication data they have from people that the previous two steps of investigation have identified as persons of interest.
- In turn pass on any information gained about these hacking activities to these countries
- Interfere with the security of websites known to be used as «information dumps» to journalists, hosted both on your territory and abroad, and to monitor these to see if the compromised emails are uploaded there – the hope is to identify the sender.

3. Findings

Even though the scenarios will be further refined and expanded in response to the first set of answers, some interesting patterns are already emerging. Focus in this paper will be on the answers to the first two scenarios.

For all three jurisdictions, it was for at least some of the hypotheticals difficult to establish in the absence of case law whether the provisions of the relevant legislation «matched» what was described. In Finland for instance, where the Coercive Measures Act was meant to bring clarity also to new forms of technologically enhanced surveillance, it remained debatable which of the three measures described in Chapter 10 of the Act, technical surveillance of a computer or similar technical device (s. 23), technical interception (s. 16), and interception of telecommunications (s. 3) applied to the hypothetical, and how that decision impacts on the type of data that can be collected this way.

The absence of clarifying case law that can establish signposts for the open issues in statutory interpretation that the national reports flagged up is a systemic problem in surveillance law. Especially for covert measures, litigation is rare, as the parties most affected will typically not even know that they had been subject of surveillance. All three systems report significant prohibitions on ISPs for instance to inform their customers that certain types of warrants for data access have been issued. On a European level, this problems has been recognised in *Klass v Germany,* where the ECtHR justified a deviation from Article 34 of the ECHR that nor-

mally prohibits *in abstracto* challenges of practices of a state organ. The court justified this departure through the difficulties that arise from the inherently secret nature of surveillance, which make it near impossible for an individual to «point to any concrete measure specifically affecting him.»[12] This is especially the case where individuals are not «subsequently informed of the measures taken against them» – as this makes it nearly – «impossible for the applicants to show that any of their rights have been interfered with.»[13]

In the UK this problem has been acerbated since the Interception of Communications Act 1985, which introduced a general prohibition to submit evidence from communication interception at trial. This is made explicit in the Investigatory Powers Act sec. 56, which states that evidence gathered by intercepting communications can't be used in court. This includes doing anything that «tends to suggest that any interception-related conduct has or may have occurred or may be going to occur». This is one of the findings where the stakeholder analysis described above is likely to produce relevant further elucidation, since this particularity of the UK approach seems difficult to explain within the systematic of the common law procedural system, where exclusionary rules of evidence have been traditionally also used to «discipline» the police and act as a deterrent against the overreach of the state. The elimination of an entire type of evidence from adversarial scrutiny seems to sit ill at ease with this organisational principle, and is possibly due to a conflict between the interest of law enforcement and security services, the latter prevailing with successive governments both on the right and left of the political spectrum.

This again is likely to be a particular problem for common law systems that rely more extensively on the ability of courts to pragmatically solve specific problems in the absence of clear legislative guidance. While this will be subject to the next reiteration of the hypotheticals, the three national reports at present do show a much greater willingness of the Finnish and Norwegian answers to speculate about likely interpretations on the basis of first principles, using also the European human rights framework to fill any gaps. This is in line what one would predict, given the usual macro-comparative analysis of the structural differences between common law and civil law jurisdictions – lawyers trained and cognitively shaped within code based systems operate under the implicit assumption that even for entire novel problems, an answer can be found in the code, if necessary by going back to general principles. Common law lawyers by contrast emphasise the role of the judiciary in developing the law and by closing gaps. They are therefore more accepting of the possibility that at a given point in time, certain questions can't be answered before the courts produce an on-point precedent. While in practice these differences are more nuanced, the answers by the national experts so far confirm these intuitive differences in attitude when confronted with novel technological challenges. For the UK, this however poses a problem – rules against the use of surveillance evidence in court, together with more widespread use of non-public procedures in terrorism related offences, the intrinsic problem of bringing legal challenges against surveillance by targeted citizens deprives the common law of its «oxygen», the cases that are needed to adjust, develop and complement the law. Where civilian and Nordic systems can fall back under these conditions on first principles, including those enshrined in European human rights law, this road is less straightforward for the common law system to take.

This can also in part explain the different level of complexity in the relevant legislation. The Investigatory Powers Act 2016 has 272 provisions, read together with 10 «Schedules» and, authorised and demanded by these, a number of «Codes of practice» of considerable length. The Coercive Measures Act by contrast, even though it regulates a much broader area, is comparatively short. However, as the UK answers to the question show, the attempt to regulate in such detail that the need for «high level» gap filling is rendered unnecessary failed, and as technology advances will continue to create cracks in the regulatory framework. Absence of litigation together with overly complex and technical legislation, much of it hidden in lengthy Codes of Practice,

12 Klass v Germany App no 5029/71 (Commission Decision, 9 March 1977) p 27.
13 ibid n 199.

creates in turn problems for the legitimacy of the regulatory framework, making it more difficult for citizens to develop awareness of the level of surveillance that they may be facing. This, we predict, should bear out in the comparative user questionnaire analysis.

The underlying problem has however already had an impact on the developing regulatory landscape. In one of the few cases that came before the Investigatory Powers Tribunal («IPT») in 2014, a group of NGOs challenged the legality of programs exposed by Snowden, such as PRISM and Tempora.[14] The case revealed that the government assumed a very broad definition of «external communications» that included interactions with foreign internet servers.[15] User engagement with the likes of Facebook or Google can constitute «overseas» communications, even when accessed domestically and perceived by citizens as a purely «domestic activity» as is the case for documents stored on cloud-based servers outside the UK. This, obviously, has repercussions for any question about legitimacy of surveillance powers, something that has also been recognised by the Strasbourg court, which had in previous decisions involving the UK laid down general guidance on the minimum requirements for legitimate surveillance practices. *Malone v UK*, *Khan v UK*, and in particular *Kennedy v UK* clarified that any surveillance methods must be «in accordance with law», and for this purpose, the measures must satisfy three requirements. First, «the impugned measure must have some basis in domestic law». Second, the relevant domestic law must be «compatible with the rule of law and accessible to the person concerned». Third, «the person affected must be able to foresee the consequences of the domestic law for him».[16]

In *Liberty and others v GCHQ,* the Tribunal sided with the plaintiffs against the government, at least in principle, ruling that at the time when the impugned exchange of surveillance data between the UK and US had taken place, there had been insufficient knowledge by citizens about the surveillance practices to meet the Kennedy test. However, it also ruled, somewhat paradoxically, that the very process of litigation before the Tribunal had now created sufficient public awareness so as to render any *future* activity along the same lines permissible. In reaching this decision, the Tribunal also watered down substantially the Kennedy test. The IPT held it was sufficient that «appropriate rules or arrangements exist and are publicly known and confirmed to exist» as long as these rules are «sufficiently signposted, such as to give an adequate indication» of their content.[17] «Domestic law» in *Kennedy* becomes a much broader reference to formal laws and other «arrangement», while the reference of the Strasbourg Court to the rule of law is altogether deleted. The rule of law requirements of clarity and openness could then be dispensed with, in favour of mere «arrangements» that are «publicly known and confirmed to exist», however ambiguous or difficult to access any «signposts» as to their content may be. As we saw, this raises both practical issues – practical issues, as it is difficult for laypeople to know what the law says, but also theoretical problems as it may even be impossible for legal experts to determine in the absence of further clarifying case law what the correct legal assessment would be.

There are no corresponding decisions in Norway or Finland, but the more principle-based approach of legal reasoning that informed the answers to the hypotheticals, indicates that we face a potential divergence between the UK and the Nordic jurisdictions in their implementation of ECHR decisions, with the UK following a more formalistic approach which, paradoxically also undermines traditional common law safeguards, while Norway and Finland aim at a more substantive implementation.

Liberty v GCHQ had been about the circumvention of domestic legal safeguards through international police collaboration. This also had a bearing on a second emerging pattern is the way in which the question of extraterritoriality in the first hypothetical was conceptualised in the three answers. All three jurisdictions have identified the need to regulate explicitly for data collected from abroad (as opposed to «merely» exchanged

14 *Liberty and others v GCHQ* [2014] UKIPTrib 13_77-H.

15 *Liberty v GCHQ*, ibid, [97]. Also confirmed in the ISC report (n 634) para 109.

16 Kennedy v United Kingdom (2011) 52 ECHR 4 at 151.

17 *Liberty and others v GCHQ* at 41.

with foreign services). All three jurisdictions have also established explicit rules for what in UK parlance is «equipment interference», i.e. clandestine hacking carried out by investigatory agencies. Where gaps arise is however the intersection between these two issues. This highlights how in the mobile Internet, old metaphors about cyberspace that informed legal responses have become overstretched. In the static Internet of old, a central question was whether a target device was stationed on private premises or in public, such an Internet cafes. With mobile phones and other Internet of Things devices that operate across a range of locations and contexts, this distinction is increasingly precarious, as our hypothetical demonstrates. Despite this, the distinction between «premises» and «public spaces» still informs in varying degrees all three jurisdictions. Consequently, all three countries indicated that the absence of clear regulation and domestic case law makes answers difficult. The responses from Norway and Finland relied in their response again on overarching general principles, including ECHR jurisprudence on Art 8, while the UK answer emphasised the unresolved nature of the issue.

As noted above, the «domestic vs foreign» dichotomy played also in the political arena a significant role in creating if not legitimacy, then public acceptance in surveillance powers. Surveillance of «foreigners» so the political rationale, seems much less problematic to legislate for. In a European setting however, at least some of these foreigners will be citizens and on the territory of other member states, which could crate not just a two-tier system of protection, problematic enough as it is for a principled approach to privacy as a human right, but a three tier system that also creates differential levels of protection between types of EU citizens.

The IP Act states that the main purpose of bulk interception is «the interception of overseas-related communications.»[18] «Overseas-related communications» are defined as communications sent or received by individuals outside the British Islands.[19] However, this distinction is a difficult one to maintain in the digital age where the «global nature of the internet» means that even domestic communications are often routed outside the UK.[20] This fact led the Joint Committee on the Draft IP Bill to conclude that the «limitation of the bulk powers to ‹overseas-related› communications may make little difference in practice to the data that could be gathered under these powers».[21] In a European setting however, this already precarious solution is further complicated, At least some of these foreigners will be citizens of and resident on the territory of other member states, which could create not just a two-tier system of protection, problematic enough as it is for a principled approach to privacy as a human right, but a three-tier system that also distinguishes levels of protection afforded to different groups of European as well.

In their answers to the variation of hypothetical 1 that let our suspect cross international borders with a mobile computing device that had been compromised for surveillance purposes, all three countries indicated as yet unresolved legal issues. Equally, all three made references to mutual legal assistance treaties (MLATs) as the most appropriate legal mechanism. However, only Norway and Finland relied in their answer on Art 40 of the Schengen Agreement, which provides probably the clearest indication of how this type of surveillance can be conceptualised so that on the one hand, jurisdictional borders do not pose undue burdens on police operations, but on the other no «blind spots» for the protection of the rights of the suspect are created. Article 40 of the Schengen Convention 1990 (CISA) concerns certain forms of surveillance conducted by police officers on the territory of another contracting party. According to Art. 40, officers of one of the contracting parties who, as part of a criminal investigation, are keeping under surveillance in their country a person who is presumed to have participated in an extraditable criminal offence is authorised to continue their surveillance in the territory of another contracting party. It is, however, a condition that the latter has authorised cross-border surveillance

18 IP Act, s 136(2)(a).

19 Ibid, s 136(3).

20 Joint Committee on the Draft Investigatory Powers Bill, *Legislative scrutiny: Draft Investigatory Powers Bill* (2016, HL 93, HC 651), para 323.

21 Ibid.

in response to a request for assistance made in advance. For obvious reasons, this provision was not available to the UK rapporteur as basis for an analogical analysis, the UK not being a Schengen member.

As a result we find a certain divergence in the way geographical borders are treated in cyberspace investigations, and the conceptual toolbox available to ensure their legitimacy, between the UK and most other European countries, a divergence that is likely to be deepened after Brexit, whatever form it will eventually take. It could however also be indicative of an even more substantive divergence. In the US, the case of *Microsoft Corp. v. United States*[22] centred around two different ways in which one might conceptualise seizure of data from servers abroad. Under one understanding, the «place» where the enforcement action takes place is the place where the data is physically located. This will then normally require to observe the formal requirements of a MLAT request to whatever county hosts the server. Conversely, one can focus at the physical location where law enforcement first gets access to such data – this will in many cases render MLAT's unnecessary, if the company owning the server also has a presence in the investigating jurisdiction. This, in a nutshell, was the interpretation of the US law enforcement agencies. One problem with this approach was that at least for the US, this could mean that certain surveillance targets were left without any adequate legal protection, falling between the chairs of 4th Amendment protection (available only for actions on US soil) and whatever protection the country where the server is hosted required. The CLOUD Act (Clarifying Lawful Overseas Use of Data Act) which came into force on the 23.3 2018 resolved this issue and rendered the litigation moot. It enshrined in law a specific understanding of Internet technology and data flows, turning what could be seen as an issue that crosses jurisdictional borders into a purely domestic process. It also tries to ensure though that adequate procedural safeguards remain in place.

This «reading», or way to conceptualise, data access is born out of frustration with the often cumbersome and time intensive MLAT process, which could not cope with the speed by which data can be destroyed or transferred. The EU reacted to the CLOUD Act through a number of proposals to facilitate the MLAT process and the cross-border gathering of digital evidence. The proposed Regulation on European Preservation Order and on European Production Order introduces new rules to help authorities secure and obtain electronic evidence stored by service providers, irrespective of where the evidence is stored. The rules will build on existing principles of mutual recognition between Member States. The European Production Order will allow a judicial authority in one Member State to request access to electronic evidence directly from a service provider's legal representative in another Member State, which will be obliged to respond within 10 days, and within 6 hours in cases of emergency. The European Preservation Order will allow judicial authorities in one Member State to oblige a service provider or its legal representative in another EU country to prevent electronic evidence from being deleted before their production request is completed.

Both approaches are built around very different «visions» of surveillance and online data gathering. Both try to maintain internal normative consistency, and with that legitimacy, also in the way protective regimes are built around surveillance powers, expressing both different historical approaches to surveillance legislation, and also differences in the respective digital economies, with the US benefiting from domestic presence of all major platform providers. The answers by the Norwegian and Finnish «fit» conceptually to the proposes «fast MLAT model» proposed by the EU. The answers of the UK however indicate that following the US lead remains a possibility – something that would become even more attractive if the UK were to be excluded from the emerging cross-border investigatory ecosystem that the EU envisages. While this could create tensions in UK-EU relations, both approaches have an internally consistent approach to human rights protection, so do not on their own answer the question what makes surveillance practices legitimate. Apart from the shared common law environment, the absence of historical experience of abuse of surveillance by dictatorships, and the general high level of social trust that is placed in judicial oversight, make such an alignment far from implausible.

[22] *In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation.*

Rather, the danger would be to follow a US based system, but without CLOUD Act or 4th Amendment, or the EU approach, but with a purely formalistic understanding of its underpinning human rights law.

The answers to the hypotheticals indicate different, mutually consistent ways in which the issue of «border» is conceptualised in different legal systems, following at least roughly the familiar lines of common law vs continental European law. Explanations for this divergence come from both the path trajectory of the respective legal mindsets as from more recent experience with dictatorial regimes. The next stage of the project will be to interrogate these different approaches through the prism of «legitimacy», looking at the political processes that shaped the legal environment, and the way in which citizens adjust their behaviour on the basis of what they know, or do not know, about their own exposure.

4. Literature

Götting, Horst Peter/Schertz, Christian/Seitz, Walter Handbuch des Persönlichkeitsrechts. München: Beck, 2008.

Legrand, Pierre, European legal systems are not converging. International & Comparative Law Quarterly, *45*(1), 1996 52-81.

Linarelli, John, The economics of uniform laws and uniform lawmaking. *Wayne L. Rev.*, *48*, 2002, 1387-1449.

Rauhofer, Judith/Abel, Wiebke/ Brown, Ian, A First Look at the Constitutional and Legal Implications of the Data Retention and Investigatory Powers Act 2014, SCRIPTed, 11 2014, 320-329.

Richards, Neil M/Solove Daniel, Privacy's other path: recovering the law of confidentiality. Geo. LJ 96 2007, 123-183.

Schafer, Burkhard. Surveillance for the masses: the political and legal landscape of the UK Investigatory Powers Bill, Datenschutz und Datensicherheit 40 2016, 592-597.

Schlesinger, Rudolf, Research on the General Principles of Law Recognized by Civilized Nations. American Journal of International Law 51, 1957 p.734-753.

Zweigert, Konrad/Kötz, Hein, Einführung in die Rechtsvergleichung auf dem Gebiete des Privatrechts. Mohr Siebeck 1996.