Swedish police implementation of IMSI-catchers in a European law perspective

Article · August 2016

DOI: 10.1016/j.clsr.2016.07.006

1 author:

Markus Naarttijärvi
Umeå University
13 PUBLICATIONS **9** CITATIONS

SEE PROFILE

SWEDISH POLICE IMPLEMENTATION OF IMSI-CATCHERS IN A EUROPEAN LAW PERSPECTIVE

*Markus Naarttijärvi**

LL.M, LL. D, Senior lecturer

Umeå University, Department of Law

90187, Umeå, Sweden

markus.naarttijarvi@jus.umu.se

Abstract:

In this article the qualitative requirements of legality under the European Convention on Human Rights are analyzed as they apply to the use of 'IMSI-catchers' – a technical device to track the location and use of cell-phones. The implementation of IMSI-catchers in the Swedish police is used as a case study and litmus test to illustrate how domestic law may interact with the requirements under convention law in this area. The article shows that the Swedish implementation of IMSI-catchers in substantive law has lagged behind the actual use of the measure in police work through references to the domestic legal principle that 'the ether is free' that serve to preclude legal protection of confidentiality of radio communications. The application of this principle highlight deficiencies in the conformity of Swedish law with both the EU ePrivacy directive and the requirements of legality under the European Convention.

Keywords:

IMSI-catcher, Surveillance, Police, Legality, Obscurity, Law, Sweden, ECHR, Ether

This manuscript has been accepted for publication in Computer Law & Security Review, the final publication is available at Elsevier. doi:10.1016/j.clsr.2016.07.006

Table of Contents

1 INTRODUCTION

Law enforcement surveillance of electronic communication is usually reliant on assistance by the service providers (or operators) of the networks where such communication takes place.[1] Through laws on communications interception, these service providers have been given the legal obligation to enable and assist interception when law enforcement agencies can show that that the legal requirements are by reference to a relevant legal authorization.[2] Service providers rarely have a vested interest in allowing authorities to eavesdrop on their customers. In fact, adapting their systems and maintaining a constant readiness to assist interception requests or requests for records or historical data is a costly affair that is likely to have no economical or competitive upside.[3] As such, establishing legal rules to require telecommunication providers to assist authorities has likely been a necessary precondition for effective surveillance of such networks.

Beyond the practical need to create access to data only available in networks belonging to private actors, such legal rules are likely to have had other functions as well, by legitimizing the interference with privacy that surveillance entail. It is by now well established that the European Convention on Human Rights (ECHR), as interpreted by the European Court of Human Rights (ECtHR) require that government measures that encroach on the right to privacy under article 8 of the convention must have a basis in law, and that this legal basis must be sufficiently foreseeable, clear, and limit government discretion.[4]

---

[1] See DeNardis L, *The global war for Internet governance* (Yale University Press 2014), p. 13.
[2] In Sweden, such assistance is required through chapter 6, section 19 of the Electronic Communications Act, whereby the operating of electronic communications networks shall "be conducted so that decisions on secret interception of electronic communications and covert surveillance of electronic communication can be implemented and so that the implementation is not disclosed" (authors translation).
[3] A study commissioned by the Swedish Telecommunications Authority found that the costs carried by service providers relating to the adaption of communications systems for surveillance between 1994 and 2004 was 215 million SEK (roughly 20 million euros), with costs estimated to increase by 40% in the following years, see Hovmark J and Jacobsson F, 'Marknadsundersökning avseende hemlig teleavlyssning m.m.' (NetLight 2005). The costs for the telecommunications industry of implementing the European data retention directive in Sweden was estimated at 220 million SEK, see Government bill (2010/11:46) Lagring av trafikuppgifter för brottsbekämpande ändamål – genomförande av direktiv 2006/24/EG, (Swedish government 2010), p. 63-68.
[4] See below, chapter 3 for a further analysis.

Consequently, there is likely to have been a certain synergy between the normative requirements established by the ECHR and the practical reality that legal mandates are necessary to enable surveillance in private networks. The question is: What happens when the assistance of telecommunications providers is no longer necessary for surveillance? When police authorities gain access to direct and unmediated means of surveillance – will legality remain a priority?

In this article, the legality requirement of the ECHR will be analyzed as it relates to IMSI-catchers, a surveillance technology that can covertly locate and gather metadata from a large number of mobile devices within a certain range without the involvement or assistance of mobile network providers.[5] This technology is of particular interest as it has been described as 'direct and unmediated', requiring no involvement by service providers.[6] Furthermore, it is a method that can be described as obscure, as many details of its practical use and legal basis in many jurisdictions is unclear,[7] which highlights the issue of legality.

In order to not only analyze the requirements, but also the impact of ECHR law in this context, the implementation of IMSI-catchers by the Swedish police authority will be analyzed. This case-study further serves to highlight the interaction between domestic law, convention law and EU law as it applies to IMSI-catchers. In this context Sweden makes for an interesting case-study for three primary reasons. First, Sweden has a tradition of transparency with regards to public documents and government action as well as a tradition of a well documented legislative process with detailed official reports as a foundation for legal bills and subsequent legislation.[8] Consequently, official documents regarding the use of IMSI-catchers can be expected to be more available and accessible. Second, the convention

[5] See below, chapter 2.
[6] Pell SK and Soghoian C, 'Your secret stingray's no secret anymore: The vanishing government monopoly over cell phone surveillance and its impact on national security and consumer privacy' (2014) 28(1) Harvard Journal of Law & Technology, p. 17, see further below chapter 2.
[7] See further below, chapter 2.
[8] See Sterzel, F, in Jonsson Cornell A (ed), *Komparativ konstitutionell rätt* (2nd edn, Iustus, Uppsala 2015), p. 79; Bull T, 'Judges without a court : judicial preview in Sweden', *The legal protection of human rights - sceptical essays* (Oxford university press 2011) 392–409, p. 393.

has a strong position in the Swedish constitution,[9] and the requirements of legality in the ECHR also exist as a general principle of Swedish law, especially in relation to government powers affecting individual rights.[10] As the Swedish principle of legality is also more formal – requiring an explicit legal basis in positive law – there should be a strong normative basis for establishing specific rules relating to IMSI-catchers. Sweden is also a state with a reputation for promoting and upholding human rights.[11] Third, the legal mandates for electronic surveillance have recently been subject to review and can thus be expected to take into account recent technological developments.[12] As such there have been both cause and opportunity for the Swedish legislator to implement legal rules on IMSI-catcher use.

This article is divided into four parts. First, the general functions and common use scenarios of IMSI-catchers are established through an analysis of open sources, government reports and available research. Second, an analysis is made of the law of the ECHR as it pertains to the types of surveillance IMSI-catchers implies. Third, the implementation of IMSI-catchers within the Swedish police authority will be described and then analyzed through an application of convention law and EU-law. Fourth and finally some general conclusions regarding the implications for privacy and protection of communications in relation to unmediated methods of surveillance will be made.

2 IMSI-CATCHERS GONE WILD

2.1 What is an IMSI-catcher?

Very briefly put, the term 'IMSI-catcher', refers to a type of electronic surveillance equipment that collects information about nearby mobile devices. This is done either

[9] The convention has a semi-constitutional status through chapter 2 section 19 of the Swedish constitutional 'instrument of government' ('Regeringsform') (1974:152), stating that laws may not be enacted contrary to Swedens obligations under the ECHR.
[10] Chapter 2, section 20 of the instrument of government, 'Regeringsform' (1974:152).
[11] See generally Hirschl R, 'The Nordic counternarrative: Democracy, human development, and judicial review' (2011) 9(2) International Journal of Constitutional Law 449–469.
[12] See generally Swedish government official reports (SOU 2012:44) 'Hemliga tvångsmedel mot allvarliga brott', (Swedish government 2012).

passively, by intercepting the radio signals already being transmitted between a mobile device (such as a mobile phone) and a mobile base-station (cell tower); or actively, by presenting itself to nearby mobile communication devices as a legitimate mobile base-station, thereby fooling devices to connect to the IMSI-catcher itself allowing further interception of information from the devices.[13]

The purpose of an IMSI-catcher is to collect certain information about nearby devices such as the 'IMSI-number'[14] identifying the device, its operator, and its subscriber. In the case of active IMSI-catchers, it may also gather information about communication taking place from the devices.[15] The specific range and capabilities of IMSI-catchers depend on the model being used and the portability also varies, from models fitting in a briefcase to models intended for installation in cars, planes or drones.[16] The capability of some more advanced IMSI-catchers allows law enforcement agencies (and others with access to the equipment) to identify nearby mobile devices (within a distance of roughly 200 m to 2 km depending on the portability of the IMSI-catcher), thereby possibly establishing the proximity of their associated owners, locate the devices with relative precision, gather communication metadata from those same mobile devices when they are used for communication, and block communication originating from the device.[17] Some models, sometimes referred to as 'DRT-boxes' or 'Dirtboxes' also enables interception of the *content* of communication originating from the mobile device.[18]

---

[13] Pell SK and Soghoian C (2014), p. 11-12; Hosein G and Palow CW, 'Modern safeguards for modern surveillance: An analysis of innovations in communications surveillance techniques' (2013) 74 Ohio State Law Journal 1071, 1081; United States Department of Justice, 'Policy Guidance: Use of Cell-Site Simulator Technology' (3 September 2015) <https://perma.cc/K99L-H643> accessed 1 April 2016.
[14] An IMSI-number is a number which consists of three separate identifying numbers, a 'Mobile country code' (issued by ITU), a 'Mobile network code' (issued by national regulatory authority) and a 'Mobile subscriber identification number' (set by the network operator), see Geir M Koien, 'An Introduction to Access Security in UMTS' (2004) 11 IEEE Wireless Communications 8.
[15] Pell SK and Soghoian C (2014), p. 9-12; Hosein G and Palow CW (2013) p. 1081.
[16] Ibid
[17] Ibid
[18] Barrett D, 'Americans' Cellphones targeted in secret U.S. Spy program' *Wall Street Journal* (14 November 2014) <http://www.wsj.com/articles/americans-cellphones-targeted-in-secret-u-s-spy-program-1415917533> accessed 27 January 2016

Even though capacities differ, it is clear that using an IMSI-catcher *may* – depending on the model used – give law enforcement agencies access to some, if not all, of the information that a traditional interception warrant would provide.[19] Some significant differences are however worth noting. Whereas an interception warrant could be used to compel the cooperation of a relevant communications provider (such as an operator of a mobile phone network to which the target subscribes), an IMSI-catcher can be deployed without the communications providers' knowledge or involvement. Pell and Soghoian has thus termed this type of surveillance 'direct' and 'unmediated'.[20] Meanwhile, a traditional warrant allows law-enforcement agencies to intercept communications metadata or content from the comfort of the office, whereas IMSI-catchers will only work in relative proximity of a target. Also, while traditional interception is most commonly targeted (signal intelligence notwithstanding) to a specific individuals' phone or computer, an IMSI-catcher is significantly more indiscriminate in the sense that it scoops up the same data from all nearby mobile devices that connect to it. Even when used to target a specific phone, the IMSI-catcher will initially gather data relating to all nearby phones in order to identify the target phone.[21] By installing an IMSI-catcher in a moving car or a plane, this gathering of information can scale from localized to large scale.[22]

2.2 Important distinctions

From both a technical and (as will be elaborated later) a legal perspective, it is necessary to distinguish between the previously mentioned *active* and *passive* IMSI-catching equipment. Strictly speaking, a passive IMSI-catcher simply listens to nearby signals and

[19] In this context 'traditional interception' refers to the use of an interception warrant by a law enforcement agency to compel a service provider to enable the interception of the communications of one service user.
[20] Pell SK and Soghoian C (2014) p. 17.
[21] United States Department of Justice, 'Policy Guidance: Use of Cell-Site Simulator Technology' (3 September 2015) <https://perma.cc/K99L-H643> accessed 1 April 2016.
[22] See Barrett D, 'Americans' Cellphones targeted in secret U.S. Spy program' *Wall Street Journal* (14 November 2014) <http://www.wsj.com/articles/americans-cellphones-targeted-in-secret-u-s-spy-program-1415917533> accessed 27 January 2016; Pell SK and Soghoian C (2014), p. 11; Hosein G and Palow CW, (2013), p. 1081.

takes advantage of the initial and unencrypted signals from nearby phones trying to establish contact with a legitimate mobile base station to register which IMSI-numbers are being broadcasted. Active IMSI-catchers on the other hand sends out signals to nearby phones, purporting to be a legitimate base station belonging to their service provider.[23] This active approach enables the equipment to gather information from phones even when they are not actively used and can, depending on the configuration 'entice' the phone to route communication through the IMSI-catcher allowing further collection of communication metadata.[24] Notably, active IMSI-catchers takes advantage of inherent security flaws in the mobile network infrastructure and essentially conducts what is known as a 'man in the middle' attack.[25] This has led some researchers to the conclusion that the use of such equipment is illegal within the European Union even when used for limited purposes such as search and rescue.[26]

2.3 Common use scenarios

Documented use of IMSI-catchers trace back to 1996 when what is believed to be the first device of this type was manufactured by a German company.[27] Devices of the same type were soon manufactured by other companies and is known to have been put into use by law enforcement[28] in the United States in the late 90s when a passive IMSI-catcher was (somewhat famously) used to locate the infamous hacker Kevin Mitnick.[29]

---

[23] See United States Department of Justice, 'Policy Guidance: Use of Cell-Site Simulator Technology' (3 September 2015) <https://perma.cc/K99L-H643> accessed 1 April 2016: "cellular devices in the proximity of the device identify the simulator as the most attractive cell tower in the area and thus transmit signals to the simulator that identify the device in the same way that they would with a networked tower".
[24] Pell SK and Soghoian C (2014), 9-12; Hosein G and Palow CW (2013), p. 1081.
[25] Desmedt Y, 'Man-in-the-Middle Attack' in Henk CA van Tilborg and Sushil Jajodia (eds), *Encyclopedia of Cryptography and Security* (Springer US 2011) <http://dx.doi.org/10.1007/978-1-4419-5906-5_324>; Meyer U and Wetzel S, 'A man-in-the-middle attack on UMTS' (ACM Workshop on Wireless Security (WiSe 2004)); Řezník T, Horáková B, and Szturc R, 'Advanced methods of cell phone localization for crisis and emergency management applications' (2015) 8(4) International Journal of Digital Earth 259–272
[26] Řezník T, Horáková B, and Szturc R, (2015) p. 259–272.
[27] Pell SK and Soghoian C (2014), p. 13.
[28] The use of similar equipment by military and intelligence agencies is more difficult to ascertain. See Pell SK and Soghoian C (2014), p. 13 (note 59).
[29] Pell SK and Soghoian C (2014), p. 14.

As described above, IMSI-catchers have many different potential functions. However, the attraction of the equipment to law-enforcement agencies generally revolve around a few primary usage scenarios; 1) locating the IMSI-number of a mobile device used by a suspect thus allowing traditional interception to take place,[30] 2) locating or establishing the presence of a suspect's known mobile device at a particular location,[31] or 3) selectively blocking devices or dialed numbers.[32]

However, even though the above mentioned functions are the most commonly mentioned, the technology has a more troubling potential. Deploying an IMSI-catcher next to a protest, demonstration or political meeting will, for instance, allow the user to track who is present (by association to their mobile device), and potentially who they communicate with.[33] Long term installation next to a political headquarter, office of a newspaper, place of worship, corporate headquarter, etc. similarly may allow for a comprehensive mapping of who visits and potentially with whom they communicate. Indeed, in Norway, covert use of IMSI-catchers near government buildings, banks and corporate headquarters in the capital has been reported, sparking fears of foreign intelligence gathering and corporate espionage.[34] Similarly in Sweden, a prominent newspaper reported having detected the use of IMSI-catchers near the government headquarters in Stockholm.[35] The use of IMSI-catchers to monitor participants in

[30] Swedish Government Official Reports, 'SOU 2010:103 - Särskilda Spaningsmetoder, Betänkande av Polismetodutredningen' (Fritzes 2010), 300; Pell SK and Soghoian C (2014), p. 21; United States Department of Justice, 'Policy Guidance: Use of Cell-Site Simulator Technology' (3 September 2015) <https://perma.cc/K99L-H643> accessed 1 April 2016.
[31] Swedish Government Official Reports, 'SOU 2010:103 - Särskilda Spaningsmetoder, Betänkande av Polismetodutredningen' (Swedish Government 2010), 296; *State of Maryland v. Kerron Andrews* [2016] Maryland Court of Special Appeals 1496; United States Department of Justice, 'Policy Guidance: Use of Cell-Site Simulator Technology' (3 September 2015) <https://perma.cc/K99L-H643> accessed 1 April 2016.
[32] Pell SK and Soghoian C (2014), p. 18.
[33] See Swedish Government Official Reports, 'SOU 2010:103 - Särskilda Spaningsmetoder, Betänkande av Polismetodutredningen' (Swedish Government 2010), 296, 301; Hosein G and Palow CW (2013), p. 1099-1100.
[34] Andreas Bakke Foss, Anders Johansen and Fredrik Hager-Thoresen, 'Secret Surveillance of Norway's Leaders Detected' (*Aftenposten*, 16 December 2014) <http://www.aftenposten.no/nyheter/iriks/Secret-surveillance-of-Norways-leaders-detected-7825278.html> accessed 27 January 2016; Anders Johansen, Andreas Bakke Foss and Fredrik Hager-Thoresen, 'New Report: Clear Signs of Mobile Surveillance in Oslo, despite Denial from Police Security Service' (*Aftenposten*, 26 June 2015) <http://www.aftenposten.no/nyheter/iriks/New-report-Clear-signs-of-mobile-surveillance-in-Oslo_-despite-denial-from-Police-Security-Service-8071885.html> accessed 27 January 2016.
[35] Kristoffer Örstadius, 'Misstänkt spioneri mot Regeringen' *Dagens Nyheter* (18 December 2014).

protests and demonstrations has been alleged in the United States,[36] as well as in the United Kingdom.[37] Though largely unconfirmed, these reports highlight, if nothing else, how covert surveillance technologies may induce rumors and fears. It also illustrates the potential use of the method if left unregulated.

The ability of IMSI-catchers to selectively monitor large crowds has special human rights implications. As Hosein and Palow puts it; '[the] ability to identify secretly and accurately every member of a crowd, via their phone's identifier, goes beyond what government authorities traditionally have been able to accomplish'.[38] As such, this particular potential of IMSI-catchers implies that such use of the equipment goes beyond the initial invasion of privacy of those subject to surveillance to further interfere with other rights such as freedom of association, religion and expression. This effect on 'neighboring' rights has also been highlighted with similar means of surveillance such as 'cell-tower dumps' where law-enforcement agencies requisition information from telecommunication providers about what phones have been connected to a certain cell-tower at a certain time.[39] Cell-tower dumps are however generally less precise as they cover a larger area and scoops up more irrelevant identifiers than the use of IMSI-catchers.[40]

Unlike traditional interception, and due to its direct and unmediated character, the detected use of an IMSI-catcher is difficult to attribute to any particular actor, which also makes it difficult to ascertain if government agencies, foreign actors or private parties are responsible for any alleged surveillance. Indeed, the availability of IMSI-catchers on the open market has been rightly described as the loss of a government monopoly on cell phone surveillance.[41]

---

[36] Hosein G and Palow CW (2013), p. 1099-1100.
[37] Ben Bryant, 'VICE News Investigation Finds Signs of Secret Phone Surveillance across London' (*Vice News*, 14 January 2016) <https://news.vice.com/article/vice-news-investigation-finds-signs-of-secret-phone-surveillance-across-london> accessed 27 January 2016.
[38] Hosein G and Palow CW (2013), p. 1099-1100.
[39] See Naarttijärvi M, *För Din Och Andras Säkerhet : Konstitutionella Proportionalitetskrav Och Säkerhetspolisens Preventiva Tvångsmedel* (Iustus 2013), p. 421-422.
[40] Swedish Government Official Reports, 'SOU 2010:103 - Särskilda Spaningsmetoder, Betänkande av Polismetodutredningen' (Swedish Government 2010), 301.
[41] Pell SK and Soghoian C (2014).

2.4 Remaining obscurity

The purpose of this chapter has been to describe, generally and from the available open sources, some of the functions and associated issues relating to IMSI-catchers. Gradually, information on what has been a very secretive method has begun to come to light, which – while still piecemeal and sometimes unconfirmed – indicate that IMSI-catchers have become a more commonly used within law-enforcement agencies.[42] Still, obscurity abounds and in many European states reliable information on the legal basis, capabilities, as well as the frequency and scope of the use of IMSI-catchers by law enforcement is still hard to come by.

For the purposes of this article however, this same obscurity regarding the method makes IMSI-catchers a suitable litmus test to evaluate how the implementation and use of IMSI-catchers interacts with the existing human rights framework. To understand the specific legal challenges that IMSI-catchers and their remaining obscurity brings in the context of Council of Europe states, parties to the European Convention, the concept of legality under the ECHR needs to be investigated further.

3 THE NORMATIVE CONTEXT – LEGALITY AND THE ECHR

3.1 Legality under ECHR as a normative bedrock

Any law-enforcement deployment of IMSI-catchers in the jurisdiction of signatory states to the ECHR is likely to raise questions regarding the applicability of - and

[42] Brad Heath, '200 imprisoned based on illegal cellphone tracking, review finds' *USA Today* (31 March 2016) <http://www.usatoday.com/story/news/2016/03/31/200-imprisoned-based-illegal-cellphone-tracking-review-finds/82489300/> accessed 1 April 2016; Brad Heath, 'U.S. Marshals secretly tracked 6, 000 cellphones' *USA Today* (23 February 2016) <http://www.usatoday.com/story/news/2016/02/23/us-marshals-service-cellphone-stingray/80785616/> accessed 25 February 2016; Andreas Bakke Foss, 'Slik overvåker norske myndigheter mobiler i Norge' *Aftenposten* (26 January 2016) <http://www.aftenposten.no/nyheter/iriks/Overvaket-mobilaktivitetene-til-egne-borgere-i-flere-enn-35-ulike-tidsperioder-i-fjor-8331223.html> accessed 25 February 2016; Swedish Government Official Reports, 'SOU 2010:103 - Särskilda spaningsmetoder, betänkande av Polismetodutredningen' (Swedish Government 2010); *State of Maryland v. Kerron Andrews* [2016] Maryland Court of Special Appeals 1496.

requirements relating to limitations of - article 8 of the convention.[43] In signatory states, the convention article essentially establishes a minimum level of protection for both private life and correspondence (and implicitly, electronic communication). While it is possible for both domestic law, and EU-law to establish a higher level of protection,[44] the ECtHR will regard the convention as establishing the minimum standard and hold states responsible for violations.[45] This implies that convention law is a natural starting point for evaluating the legal requirements relating to the use of IMSI-catchers, before turning to domestic law or EU-law.[46]

3.2 Some initial observations on applicability of article 8 of the ECHR

The use of IMSI-catchers certainly seems to constitute a *prima facie* interference with interests that fall within the scope of article 8 of the convention. For the sake of clarity, it is still worthwhile to further analyze the extent of the information IMSI-catchers collect, and the means through which they collect it, both of which fall within the scope of article 8.

While IMSI-catchers have not yet explicitly been the subject of scrutiny by the ECtHR, the Court does not, in practice, assign decisive importance to what particular method or technology that is used for surveillance, focusing instead on the information that have been gathered and the nature and degree of interference with the applicants' private life and

[43] Art. 7 of the EU-charter of fundamental rights will in most cases be applicable simultaneously, as the confidentiality of electronic communications falls within the scope of the ePrivacy Directive (see further below, section 5.2), however as art. 7 of the charter corresponds to article 8 of the convention, the ECHR will be the focus of this analysis. Furthermore the ePrivacy directive allows for limitations of communications confidentiality only in accordance with the ECHR and the developed case law of the ECtHR.

[44] See article 52(3) and 53 of the EU Charter of fundamental rights.

[45] See *Bosphorus Hava Yolları Turizm ve Ticaret Anonum Şirketi (Bosphorus Airways) v. Ireland*, no. 45036/98 [GC], 30 June 2005; *Matthews v. The United Kingdom*, no. 24833/94 [GC], 18 February 1999.

[46] This analysis will not dive into the issue of proportionality, as this is a matter which is more dependent on the specific factual context in which the method is applied. In some matters however, it is difficult to clearly separate the analysis of the court pertaining to legality and proportionality (through the requirement that a limitation should be 'necessary in a democratic society). This is especially true in relation to available safeguards, as those safeguard may simultaneously serve to limit the discretion of state authorities (which is primarily an issue concerning legality) and serve to reduce potential abuse (thus becoming a relevant factor in a proportionality analysis).

communications. Accordingly, the Court in the *Bykov v. Russia* case found that the use of radio-transmitters which allowed authorities to listen to communications, should be evaluated following the same criteria that applied to communications interception through traditional means.[47] Any analysis of the applicability of article 8 on IMSI-catcher use must therefore take into account the dual nature of the method and analyze the capabilities of the device in the sense that it outputs certain information, as well as the method it uses to output that information. As has been established, IMSI-catchers serve not only to monitor the presence of users of mobile devices in a certain area and pinpoint their location, it also gathers identifying information about the users, their mobile devices, and possibly their communications by essentially interfering with communication pathways.[48]

In establishing the applicability of art. 8, it is initially worth mentioning that the case-law of the ECtHR relating to article 8 and the privacy of individuals in public spaces does indicate a somewhat weaker protection for certain types of government observation when there is no reasonable expectation of privacy, or when the observation constitutes only a *de minimis* interference with the privacy of the individual. For example, the mere monitoring of a person through a surveillance camera in a public setting without recording the visual data has not been seen by the ECtHR as restriction of privacy, only entering the scope of art. 8 through the recording, storing or subsequent dissemination of the surveillance footage.[49] In a similar vein, police documentation of protests in a public place was not deemed to be a privacy intrusion when the photos taken were not intended for subsequent identification of individuals or further processing.[50] The applicability of these cases to the use of IMSI-catchers is however doubtful at best, given how an IMSI-catcher operates and the purpose behind their use. Indeed, any foreseeable use of IMSI-catchers will serve to identify

[47] *Bykov v. Russia*, no. 4378/02, 10 March 2009, p. 79; 'In the Court's opinion, these principles apply equally to the use of a radio‐transmitting device, which, in terms of the nature and degree of the intrusion involved, is virtually identical to telephone tapping.'
[48] See above under chapter 2.
[49] *Peck v. The United Kingdom,* no. 44647/98, 28 January 2003, p. 59 & 63.
[50] *Friedl v. Austria,* no. 15225/89, January 1995, Series A no. 305-B, opinion of the Commission, p. 21, §§ 49-52.

individuals or their location as well as establish a basis for further processing of this information. Consequently, the relevant principles of law applicable to IMSI-catchers must instead be found in cases relating to communications metadata surveillance and geographical tracking.[51]

Before turning to the more specific case-law relating to these categories of surveillance, it is worth noting that the core principles in this context is under continuous development. The Grand Chamber of the ECtHR has recently delivered a landmark judgment against Russia relating to surveillance of mobile communication networks,[52] this was followed by a chamber judgment against Hungary,[53] both of which reiterated and to a certain extent expanded on the settled principles applicable to interception of communications *content* toward a more restrictive view on the use of such methods.[54] While it may be difficult to clearly delineate to what extent the more recently developed requirements applicable to content are equally applicable to interception of metadata, the core principles of legality as it applies to surveillance and interception are more settled, equally applicable, and more likely to remain stable. Therefore, the discussion in this chapter will focus on these core principles with only brief observations regarding recent developments. In any case, as the use of IMSI-catchers implies surveillance of telecommunication metadata, geolocation surveillance and, implicitly, some manner of data collection and retention, the relevant case-law becomes a complex interconnected web of cases relating to these contexts.

3.3 Metadata surveillance and the quality of law requirement

In 1984, the first case relating specifically to communications metadata was decided by the ECtHR. The case, *Malone v. The United Kingdom,* concerned the use of a method called

[51] The potential use of certain models of IMSI-catchers to gather communications *content* will not be the main focus of this analysis. Sufficient to say the requirements in relation to legality will be even stricter, and the proportionality of the measure will be affected.
[52] *Roman Zakharov v. Russia*, no. 47143/06, 4 December 2015.
[53] *Szabó and Vizzy v. Hungary*, no. 37138/14, 12 January 2016.
[54] Notably the Szabó and Vizzy case, while repeating most of the principles in the Zakharov case, diverted somewhat from certain terms established by the grand chamber, which was highlighted and criticized in a concurring opinion in the Szabó case by judge Pinto de Albuquerque.

'metering' by the British police, whereby the police authorities were provided with information from the phone company about numbers called by a certain subscriber, as well as the duration of the calls. The ECtHR established that government access to this type of communications information constituted a limitation of article 8 in the same vein as access to content of communications. It thus required a basis in law.[55]

This requirement that legitimate limitations or interferences with rights under the ECHR must have a basis in law is inherent in the convention itself, expressed in those articles, such as art. 8-11 where the right allows for potential limitations. From the convention text itself however, the exact extent of this requirement is uncertain. The terms 'prescribed by law' and 'in accordance with the law' could, on the face of it, contain a very limited expression of 'rule by law' where state interferences should (notwithstanding the requirements of a legitimate purpose and proportionality) either avoid violating existing law, or that they should simply have some sort of legal basis. This is however not the case, and in *Malone*, the ECtHR found that the requirement of 'in accordance with the law' included certain qualitative aspects of the law which had been developed through two earlier landmark cases, The *Sunday Times* case, and the *Silver* case.[56]

The *Sunday Times* judgment, handed down in 1979, concerned a contempt of court order that restricted the right of the Sunday Times newspaper to publish certain material. The issue at hand was not so much if there was a legal basis for such an order, but rather if this legal basis was foreseeable enough to meet the 'prescribed by law' requirement in Art. 10 of the convention.[57] The ECtHR concluded that two requirements beyond the very existence of law (enacted or judge-made) followed from the 'prescribed by law' expression. First, the accessibility of the law, allowing the individual an indication, that is adequate in the circumstances, of the legal rules applicable to a given case. Secondly, that the norm is formulated with sufficient precision to enable the individual (if need be with appropriate

[55] *Malone v. The United Kingdom* (8691/79) August 2, 1984, § 84.
[56] Ibid. § 67-68.
[57] Sunday Times *v. The United Kingdom*, no. 6538/74, 26 April 1979, p. 46.

advice) to regulate his or her conduct. This latter requirement entailed, the court found, a certain balancing between the precision of the law and the ability of the law to keep pace with changing circumstances, as absolute certainty was unattainable.[58]

The court further elaborated on these qualitative aspects in the case of *Silver and others v. the United Kingdom* which followed almost ten years later, concerning the mail control regime of a prison.[59] At the outset, the ECtHR established that despite the different wording of the legality requirement in art. 10 and art. 8 of the convention ('prescribed by law' and 'in accordance with the law' respectively), the principles established in the former context must be applicable in the latter context as well. The court then reiterated the requirements from the *Sunday Times* case, adding one significant detail – a third criterion that '[a] law which confers a discretion must indicate the scope of that discretion'.[60] It is worth noting that these elements of legality - precision and limited discretion - are to a large extent interacting, and thus difficult to conceptually keep apart as vagueness may in practice allow a greater degree of interpretation and thus implies discretion. Clear limitations on discretion conversely may serve to increase precision.

Returning again to *Malone*, the court applied the criterions developed in *Sunday Times* and *Silver* cases but found that given the special context of secret surveillance the law may not be so foreseeable as to allow the individual to foresee when the authorities are likely to intercept his or her communication. However, the law must nevertheless "be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to this secret and potentially dangerous interference with the right to respect for private life and correspondence".[61] Indeed the ECtHR found that given the secrecy surrounding communications surveillance and the associated lack of scrutiny by the public, the importance of limited discretion of the executive

[58] ibid.
[59] *Silver and others v. The United Kingdom,* no. 5947/72; 6205/73; 7052/75; 7061/75; 7107/75; 7113/75; 7136/75, 25 March 1983, § 85-95.
[60] ibid § 88.
[61] *Malone v. The United Kingdom* (8691/79) August 2, 1984, § 67.

was all the more important as an unfettered power would be contrary to the rule of law: "Consequently, the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity, having regard to the legitimate aim of the measure in question, to give the individual adequate protection against arbitrary interference".[62] Thus, while the ECtHR has accepted that certain detailed rules relating to the implementation of surveillance measures may not be available to the public through substantive law, it has continuously held that the rules indicating the scope of discretion must be.[63]

The requirements elaborated above have since then been applied and developed in cases relating to interception and surveillance of different kinds. To no surprise, where no statutory system or substantive law allowing for surveillance has existed at all the court has found a violation of article 8.[64] Similarly, where *access* to the relevant rules regulating surveillance has been limited, the court has generally attempted to analyze if the scope of the conferred powers are available to the public to allow foreseeability. While more technical and detailed aspects of surveillance may be set out in internal documents and not necessarily available to the public, the legitimacy of such internal rules will in the end depend on the capacity of those details to affect the users' right to respect for their private life and correspondence. If they do, the Court have considered that they must be accessible to the public.[65] Similarly where the government has relied exclusively on non-binding internal guidelines, the court has found a violation of the 'in accordance with the law' requirement.[66] The Court has also found a violation in cases where the basis in substantive law has been overly vague and subject to conflicting interpretations.[67]

---

[62] Ibid. § 68.
[63] *Malone v. The United Kingdom* (8691/79) August 2, 1984, § 68; *Huvig v. France*, no. 11105/84, 24 April 1990, § 29; *Leander v. Sweden*, no. 9248/81, 26 March 1987, § 51.
[64] *Taylor-Sabori v. The United Kingdom,* no. 47114/94, 22 October 2002, § 19.
[65] See *Roman Zakharov v. Russia*, no. 47143/06, 4 December 2015, § 241 where certain technical requirements unavailable to the public provided direct access of authorities to telecommunications network.
[66] See *Kahn v. The United Kingdom* no. 35394/97, 12 May 2000, §§ 27-28.
[67] See *Malone v. The United Kingdom* (8691/79) August 2, 1984, § 79-80.

Beyond the foreseeability the Court has consistently held that the relevant rules authorizing surveillance must also be compatible with the fundamental principle of Rule of Law.[68] In the context of surveillance of content, the Court has developed a set of legal safeguards that should be present in the law, to minimize discretion and avoid abuses of power and prevent the dangers associated with secret surveillance: 1) the nature of offences that may give rise to an interception order; 2) a definition of the categories of people liable to have their telephones tapped; 3) a limit on the duration of telephone tapping; 4) the procedure to be followed for examining, using and storing the data obtained; 5) the precautions to be taken when communicating the data to other parties; and 6) and the circumstances in which recordings may or must be erased or destroyed.[69]

While most aspects of legality that apply to metadata are the same as those the court has established in relation to content of communication, there are some differences. In *P.G and J.H* the court indicated that in relation to information about numbers called, the applied principles could be construed in a manner which is somewhat less strict; referring "essentially to considerations of foreseeability and lack of arbitrariness".[70] This implies that certain legal safeguards applicable to interception of content, such as the above mentioned six Rule of Law requirements from *Klass*, might not apply as strictly to numbers called. This approach by the Court has been regarded as a failure to take into account the type of information that can be gathered through metadata.[71]

In this context however, it should be noted that developments in the case-law of the European Court of Justice (ECJ) indicates a growing concern regarding the sensitivity of

[68] *Huvig v. France*, no. 11105/84, 24 April 1990, § 31.
[69] Recently reaffirmed and summarized in *Roman Zakharov v. Russia*, no. 47143/06, 4 December 2015, § 231, see also *Huvig v. France*, no. 11105/84, 24 April 1990, § 34; *Amann v. Switzerland*, no. 27798/95 [GC], 16 February 2000, §§ 56-58, *Weber and Saravia v. Germany*, no. 54934/00, 29 June 2006, § 95; and *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria,* no. 62540/00, 28 June 2007 § 76.
[70] See *P.G. and J.H. v. The United Kingdom* no. 44787/98, 25 September 2001, §§ 46-47, contrasting the case in question to *Kopp v. Switzerland*, no. 23224/94, 25 March 1998, which concerned the tapping of a lawyers phone-line, including the content of communications.
[71] See Iain Cameron in Swedish Government Official Reports, 'SOU 2010:103 - Särskilda spaningsmetoder, betänkande av Polismetodutredningen' (Swedish Government 2010), p. 477.

metadata.[72] Though uncertain, it is perhaps not unlikely that the Strasbourg court may move toward applying more rigorous standards in this context as well.[73]

3.4 Geolocation surveillance and the quality of law requirement

The legality requirements mentioned above in the context of metadata mainly apply in the case of geolocation surveillance, i.e. the collection of information regarding the whereabouts of a person, as well. However, some particularities in relation to geolocation surveillance are worth mentioning. The only case specifically dealing with this type of surveillance so far is *Uzun v. Germany*.[74] The case concerned an investigation into a suspected member of a left-wing extremist terrorist movement. To follow his movement, a GPS-tracker was installed in the car of a presumed accomplice of his, allowing authorities to determine the location and speed of the car (and by association often the suspect and his presumed accomplice) once per minute for some three months until the arrest of the suspect.[75] In determining the applicability of Art. 8 of the convention the Court did not place decisive significance to the fact that the surveillance centered on the car of the presumed accomplice, as the surveillance still allowed the authorities to continuously monitor the suspect, record his movements, draw up a pattern of his movement and collect additional evidence at the places the applicant had travelled to. Evidence that was later used in the criminal case against the suspect.[76] However according to the Court, GPS surveillance;

> *"is by its very nature to be distinguished from other methods of visual or acoustical surveillance which are, as a rule, more susceptible of interfering with a person's right to respect for private life, because they disclose more information on a person's conduct, opinions or feelings."*[77]

[72] See the judgment of the ECJ in *Digital Rights Ireland and Seitlinger and Others* (cases C-293/12 and C-594/12, 8 April 2014).
[73] References to the ECJ cases regarding the sensitivity of metadata has been made in both *Roman Zakharov v. Russia*, no. 47143/06, 4 December 2015, § 147, and *Szabó and Vissy v. Hungary*, no. 37138/14, 12 January 2016, § 23.
[74] *Uzun v. Germany*, no. 35623, 2 August 2010.
[75] *Uzun v. Germany*, no. 35623, 2 August 2010, §§ 6-13.
[76] *Uzun v. Germany*, no. 35623, 2 August 2010, §§ 51.
[77] *Uzun v. Germany*, no. 35623, 2 August 2010, § 52.

This reasoning did not however change the fact that the surveillance in question, together with the processing and use of the data obtained, amounted to an interference with Article 8.[78] Consequently the GPS surveillance had to be justified under article 8(2) and reach the established standards of legality.

In relation to the quality of law criterions, the Court acknowledged that established principles did not preclude a gradual development of the legal basis for surveillance through judicial interpretation in domestic case-law if this was foreseeable. Significance was thus placed on how domestic courts in Germany had unanimously agreed that the surveillance in the case could be based on a legal rule allowing for "other special technical means intended for the purpose of surveillance".[79] The ECtHR thus accepted that the authorizing legislation was expressed in technology-neutral[80] terms, provided that the interpretation by domestic courts in published case-law, was specific enough.[81] Consistent with its approach to metadata in *P.G. and J.H v. the United Kingdom* the ECtHR in *Uzun* saw fit to distinguish the GPS surveillance in the case from the safeguards established in relation to content, given the different nature of the privacy intrusion:

> *"While the Court is not barred from gaining inspiration from these principles, it finds that these rather strict standards, set up and applied in the specific context of surveillance of telecommunications[…], are not applicable as such to cases such as the present one, concerning surveillance via GPS of movements in public places and thus a measure which must be considered to interfere less with the private life of the person concerned than the interception of his or her telephone conversations."*[82]

Consequently, the Court found that the more basic principles of foreseeability and limited discretion was more suitable to apply in this case. While the need for prior approval of surveillance by a court was toned down, the Court did seem to place material significance to the availability of one specific safeguard in the German system; the possibility of a criminal court to review the legality of a surveillance measure and, if the measure was found to be

[78] Ibid.
[79] Ibid. § 67.
[80] For an in depth analysis of technology neutrality in law, see Chris Reed, *Making laws for cyberspace* (Oxford University Press 2012), p. 189-202.
[81] *Uzun v. Germany*, no. 35623, 2 August 2010, § 64.
[82] *Ibid*, § 64.

unlawful, exclude the evidence obtained thereby from use at the trial. This was highlighted as an 'important safeguard' which discouraged the investigating authorities from collecting evidence by unlawful means, especially in combination with a responsibility to inform the concerned person about surveillance that had taken place.[83]

3.5 Implications for IMSI-catcher use

Following this analysis of the case-law of the ECtHR the likely legality requirements applicable to IMSI-catchers may now be summarized. It is clear that neither metadata surveillance nor geolocation surveillance have been seen by the Court as comparable with interception of content in respect of the interference with the right to privacy and communications. Still, it is also established that both types of surveillance are included in the scope of article 8 and necessitates justification under article 8(2). In relation to the requirement that such measures are 'in accordance with the law' it is apparent that beyond the need for a substantive basis in law, the qualitative aspects of access, foreseeability and limited discretion have been highlighted as important. While such foreseeability may stem from continuously developed case law, it still requires that the scope of the powers and discretion given the authorities are clear. It should finally be remarked that these requirements constitute the most basic threshold of a potential justification, subject to a subsequent review of necessity and proportionality under the 'necessary in a democratic society'. However, as will be shown, states may be reluctant to meet even this basic threshold.

[83] Ibid, §§ 71-72.

4 THE EMERGENCE AND IMPLEMENTATION OF IMSI-CATCHERS IN THE SWEDISH POLICE

4.1 'A method used in nearby countries'

The first official Swedish document reference to the functions of IMSI-catchers can be found in an official report to the Swedish parliament (Riksdag) in 2005.[84] This report highlighted the increased use of refillable cash-cards for cell phones, which had made it difficult to ascertain who used a particular phone. As the report noted, criminals often use, and switch between, many different phones. According to the report, the Swedish Security Service had pointed to how 'nearby countries' made use of a particular equipment that could identify the use of a certain mobile device within a certain area. This method could, according to the authors of the report, be very beneficial in identifying relevant devices in use by a suspect and the authors of the report concluded that the use of this measure should be implemented within the existing legal framework for secret telephone surveillance in the Swedish Code on judicial procedure. This would entail that its use would be subject to a warrant by a court under the same circumstances as traditional metadata surveillance through the assistance of telecommunication providers.[85] The recommendations of the 2005 report relating to IMSI-catchers were, however, never implemented.

4.2 'A relatively large scale use'

The issue of IMSI-catchers was revisited in the second official report on police methods in 2010.[86] This report now explicitly referred to the equipment as an 'IMSI-catcher' and noted that within law-enforcement agencies existed a 'relatively large-scale use of IMSI-

[84] Swedish Government Official Reports 'SOU 2005:38 – Tillgång till elektronisk kommunikation i brottsutredningar m.m., betänkande av Beredningen för rättsväsendets utveckling', (Swedish Government 2005).
[85] Swedish Government Official Reports 'SOU 2005:38 – Tillgång till elektronisk kommunikation i brottsutredningar m.m., betänkande av Beredningen för rättsväsendets utveckling', (Swedish Government 2005) p. 208-212.
[86] Swedish Government Official Reports, 'SOU 2010:103 - Särskilda spaningsmetoder, betänkande av Polismetodutredningen' (Swedish Government 2010).

catchers'.[87] Interestingly, the report described, briefly, the technical functioning of IMSI-catchers as an equipment that:

> *[F]or very brief time presents itself as a base-station for mobile phones in its vicinity. Through this it becomes clear what IMSI- or IMEI-numbers and consequently what communications identifiers are active in the area. It is not necessary that the phone is used for a call, it is sufficient that it is powered on.*[88]

From this description, it appears that the IMSI-catchers in use by the Swedish police are active, rather than passive, as the equipment actively sends out signals to present itself as a legitimate base station.[89]

The 2010 report went on to conclude that the use of this type of measure was important for the investigation and prevention of serious crime. The use of the method up until this point had not been based on any authorization in law or internal regulations, but on a presumption that the 'ether[90] is free', a principle or tradition in Swedish law that allowed for free interception of radio signals.[91] The 2010 report came to the conclusion that although this interpretation of existing law was technically not incorrect and the use of IMSI-catchers could not be said to be illegal, there was some doubt whether the legal basis could survive future scrutiny with regards to the the legality requirement in Swedish constitution and the European Convention on Human Rights (ECHR).[92] Given this analysis, the report concluded that a

---

[87] Ibid p. 295.
[88] Ibid p. 297.
[89] See above, section 2.2.
[90] The term 'ether' (or 'æther' in this translation could be replaced with the term 'air' even though the Swedish equivalent of 'ether' is more frequently used in reference to the legal concept, see Government bill (1992/93:200) 'om en telelag och en förändrad verksamhetsform för Televerket, m.m.', (Swedish Government 1993); Swedish Government Official Reports, SOU 1992:110 – Information och den nya informationsteknologin, betänkande av Datastraffrättsutredningen', (Allmänna förlaget 1992); Government bill (2006/07:63) 'En anpassad försvarsunderrättelseverksamhet'', (Swedish government 2007) s. 67. Notably, in physics the theories regarding the existence of an æther have been superseded by general relativity although Einstein did allow for a hypothetical alternate use of the idea which could harmonize with general relativity, see Albert Einstein, 'Ether and the Theory of Relativity' in Michel Janssen and others (eds) (Springer Netherlands 2007) 1537 – 1542, see also P. A. M. Dirac, 'Is there an Æther?' (1951) 168(4282) Nature <http://dx.doi.org/10.1038/168906a0> 906 – 907.
[91] See further below section 4.4. The similarity between the wording of this principle and a common expression among Swedish kids annoyingly waving their hands in front of other kids faces exclaiming 'the air is free' is, perhaps, coincidental.
[92] Swedish Government Official Reports, 'SOU 2010:103 - Särskilda spaningsmetoder, betänkande av Polismetodutredningen' (Swedish Government 2010), p. 79-81. This analysis was likely influenced by a thorough analysis of convention law provided in an enclosed expert report to the inquiry penned by professor Iain Cameron (p. 425-493).

more foreseeable footing in law would be beneficial. Consequently, a new law on reconnaissance measures was proposed as a basis for the future use of IMSI-catchers.[93] As with the previous report from 2005, this recommendation has yet to be implemented in law.

4.3 DIY lawmaking – The internal regulation of an unregulated method

The inactivity on behalf of the Swedish legislator did however not stall further implementation and use of IMSI-catchers by the Swedish police. In 2011 the chief of what was then the Swedish *National bureau of investigation* ('Rikskriminalpolisen')[94] established an internal regulation ('Tjänsteföreskrift') on the use of certain technical methods for reconnaissance.[95] It implemented as internal requirements some of the suggestions of the 2010 official report, using the thresholds for the deployment of IMSI-catchers recommended by the report. An IMSI-catcher may according to the regulation be used to 'identify which mobile electronic equipment or other equipment for radio communication that is located within a certain geographical area'.[96] Its use is allowed provided there is suspicion of a crime for which is prescribed a prison sentence of one year or more, or, provided that the method could reasonably be believed to be beneficial for the prevention of such a crime.[97] The authority to decide on the use of the method was placed internally with the commander of the bureau of investigation, his or her deputy, or the commander of the reconnaissance unit. It could be delegated, but not below the rank of commissioner ('Kommissarie').[98] If the use of the measure was of a particularly intrusive nature the decision had to be made by the commander or his or her deputy. In case of urgency, a police officer, regardless of rank, was allowed to make an interim decision on the use of the method provided it was subject to later review by the unit commander.[99]

[93] Ibid
[94] Now reorganized under the 'Department of National Operations' (NOA).
[95] TjF 2011:5 409 - Tjänsteföreskrift om vissa tekniska spaningsmetoder 2011.
[96] Ibid, section 5.8.
[97] Ibid, section 7.
[98] Ibid, section 8.3
[99] Ibid, section 8.1; 8.2.

Some aspects of the internal regulation depart from the suggestions of the 2010 report. Notably the regulation, as it only affects the internal routines relevant to IMSI-catcher use, does not provide for the external control or oversight suggested by the report. Also, somewhat surprisingly, section 1.3 of the regulation allows for a general deviation from all requirements of the regulation, if so decided by the head of the preliminary criminal investigation within which the method would be applied.[100] In most cases where IMSI-catchers could be applied this role would be placed with a public prosecutor.[101]

Importantly, this internal regulation has not been made public nor is the existence of the regulation referenced in any legislative material, inquiries or reports published since its establishment. Requests under freedom of information laws made by this researcher for any internal regulations or guidelines, statistics or procurement decisions relating to IMSI-catchers,[102] was met with a preliminary denial as any such documents would be considered classified.[103] After a request for a definitive decision by the police authority (which may under Swedish law be appealed to a general court of law), the internal regulation was released, while the other requested information was not provided, as it was stated not to exist within the police authority.[104]

Also of note is that the authority to use IMSI-catchers conferred through the regulation is not based on any rule of law. The regulation points, through a short preamble, to the Swedish constitution, the ECHR, the Police act of 1984 and the Swedish criminal code as support for the enactment of the regulation, but does not provide any specifics to explain these references or how the regulation relates to those legal sources. Indeed, when questioned, the legal department of the police authority maintained that (as of September 2015) the use of IMSI-catchers is 'an unregulated reconnaissance method', that the internal regulation is the only legal basis for its use and that prior to the establishment of the internal regulation, there

[100] This implies that deviations from the regulation is not possible when applied in intelligence-gathering operations.
[101] Chapter 23, section 3, Swedish code of judicial procedure ('Rättegångsbalk').
[102] E-mail from author to registrator Polismyndigheten (7 May 2015).
[103] Preliminary decision ('Tjänstemannabeslut') June 24, 2015 (dnr A194.873/2015).
[104] Police authority decision ('Myndighetsbeslut') July 3, 2015 (dnr A281.788/2015).

was no legal basis for the use of IMSI-catchers.[105] This is also manifested in the fact that the recommendations made in the official reports to the Swedish Riksdag have yet to be implemented by the government.

The Swedish Police authority could not provide any information on questions such as "for how long has the method been used?" or "how often is it used?", as the requested information or statistics did not, according to the legal department, exist within the Police authority. Indeed the internal regulation was, according to the legal department, the 'only written regulation of the method'.[106] Thus the only publicly available information on the actual use of IMSI-catchers is still the 2010 report which points to a relatively large-scale use.[107] It is difficult to approximate this statement into any absolute numbers.

4.4 The principle that the 'ether is free'

The implementation of IMSI-catchers in Sweden is, as has been mentioned above, primarily based on the assumption that the 'ether is free'.[108] This assumption, often described as a 'principle' in Swedish legal material, stems from the idea that anyone should be free to receive or listen to radio transmissions and is a legacy from the Swedish radio act of 1966.[109] The logic behind this principle seems to be that in practice, it is difficult for people to control what signals are picked up by their radio receivers. Accordingly, it would be unfair to apply criminal sanctions on unauthorized individuals that listens to unencrypted signals.[110] It is thus for the sender to secure radio communications through encryption should he or she want to avoid this. This principle also underpinned the signals intelligence gathering of the Swedish Defense Radio Establishment through eavesdropping of (and decryption of) radio

[105] Email from the legal department of the Swedish police authority to author (14 September, 2015)
[106] Ibid.
[107] Swedish Government Official Reports, 'SOU 2010:103 - Särskilda spaningsmetoder, betänkande av Polismetodutredningen' (Swedish government, 2010), p. 295.
[108] See section 4.2 above.
[109] Section 3 of the 1966 radio act, Radiolag (1966:755)
[110] Government bill (1966:149) 'förslag till radiolag', (Swedish Government 1966), p. 57, see further below, section 5.1.

communications – foreign and domestic - for decades, with the legislator only stepping in to create a legal basis for interception once the eavesdropping was to be conducted in wired communications as well.[111]

The principle is also evident from a statement in the preparatory works to the Swedish penal code section on unlawful breaching of computer systems (i.e. 'hacking' or in Swedish 'dataintrång'),[112] where the government argued:

> *'Regarding data transmitted via radio, however, as a rule, the interception of such radio communications fall outside the criminalized area. It follows from the principle that the ether is free and that the unauthorized access requirement therefore can not be regarded as fulfilled'.*[113]

Accordingly, the reference to the idea that the 'ether is free' to legitimize the use of IMSI-catchers is not itself grasped from the thin air it refers to. The principle has left a footprint in legislative acts. It is subject to certain exceptions however. Returning to the Swedish preparatory works on unlawful breaching of computer systems, the government did hold that the principle that the ether is free should not apply if the radio-transmitted data are encrypted, or if the data are modified or deleted or otherwise impacted.[114] Consequently, any use of an IMSI-catchers to decrypt or impede the transmission could potentially fall within the scope of the section. As mentioned above, some IMSI-catchers allow decryption and blocking of communications and any such use of the equipment should be considered unlawful and subject to criminal sanctions.

There are other signs of the free ether having been established in Swedish law. The government has also in legal bills relating to signals intelligence maintained that the constitutional protection of the right to privacy and correspondence in Ch. 2 Sec. 6 of the Swedish Instrument of Government does not cover radio communications.[115] This claim is

---

[111] C.f. Government bill (2006/07:63) 'En anpassad försvarsunderrättelseverksamhet', (Swedish government 2007), p. 69-70.
[112] Swedish penal code ('Brottsbalk') (1962:700), chapter 4, section 9(c).
[113] Government bill (2006/07:66) 'Angrepp mot informationssystem', (Swedish government 2007), p. 49.
[114] Government bill (2006/07:66) 'Angrepp mot informationssystem', (Swedish government 2007), p. 49.
[115] Government bill (2006/07:63) 'En anpassad försvarsunderrättelseverksamhet', (Swedish government 2007), p. 69-70.

based on statements in preparatory works to the constitutional amendment establishing this right, stating that the protection does not cover 'conversations in public crowds or radio transmissions'.[116]

The analysis of existing law that has been sketched out above is, though often repeated by the government, an oversimplification. As will be shown, the principle that the 'ether is free' is in fact circumscribed by several points of law that makes it difficult to apply to the use of IMSI-catchers, or in relation to private radio communications whatsoever. In fact, one may reasonably question if the principle in itself survives closer scrutiny.

5 ANALYZING IMSI-CATCHER LEGALITY UNDER SWEDISH AND EUROPEAN LAW – FROM BAD TO WORSE?

Ascertaining the legality of IMSI-catchers under Swedish law is, to a certain extent synonymous with an investigation into the legality requirements under the ECHR. The Convention is implemented as Swedish law with a certain semi-constitutional standing through a constitutional rule stating that laws may not be enacted that violate the rights of the ECHR.[117] Also, through a constitutional rule on judicial review, courts are instructed not to apply laws violating the constitution – and implicitly, the convention.[118] Similarly, Swedish government agencies are required not to apply laws if they find that doing so would violate the constitution.[119]

As mentioned above,[120] an official inquiry did look into the use of IMSI-catchers, and in an addendum to the report of that inquiry the convention requirements relating to several different surveillance methods were thoroughly investigated. As such, the more general conclusion of the inquiry stating that 'a more solid footing in law' of the use of IMSI-catchers

[116] Government bill (1975/76:209) 'om ändring i regeringsformen', (Swedish Government 1976), p. 147.
[117] Chapter 2, section 19 of the Swedish constitution, Kunggörelse (1974:152) om beslutad ny regeringsform.
[118] Chapter 11, section 14 of the Swedish constitution, Kunggörelse (1974:152) om beslutad ny regeringsform.
[119] Chapter 12, section 10 of the Swedish constitution, Kunggörelse (1974:152) om beslutad ny regeringsform.
[120] See section 4.2 above.

would be beneficial, is correct. However, this conclusion is, to a large extent, an understatement.

It is true that the ECtHR has not authoritatively settled the exact requirements of legality, or proportionality for that matter, in relation to IMSI-catchers. Two things are however not in question. First, as has been analyzed above, the use of IMSI-catchers constitutes an interference with the right to private life and correspondence under article 8 of the convention. Secondly, any analysis of the potential legality of the use of the method must start with establishing, at least, that the method is not in fact illegal according to Swedish law. Any claim to legality, or reference to wiggle-room with regards to the exact requirements of legality, is moot if it can be shown that the use of the method is *ultra vires* under domestic Swedish law.

5.1 Putting the free ether in context

As mentioned above the origin of the principle that the ether is free can be found in the Radio Act of 1966. Section 3 of the act established a basic rule that anyone could have and use a radio receiver.[121] Indeed in the government bill, the minister in charge of drafting the law stated that in a democratic country valuing freedom of speech and freedom of information as some of the most important rights, it was obvious that anyone should have the right to have a radio receiver and listen to any *public radio broadcast* ('rundradiosändning') that he may pick up on his receiver.[122] Though this statement does indicate a preference for a certain freedom in relation to the ether, this statement, and the rules established by the 1966 act must be put into context.

Primarily, the radio act of 1966 must be understood in the light of that owning a radio receiver had, up to this point, been subject to the granting of a license by the government, something that had become impractical and untenable in the light of how common radio receivers had become. Furthermore, the freedom to listen as described in the bill refers

[121] Radio Act (1966:755).
[122] Government bill (1966:149) 'förslag till radiolag', (Swedish Government 1966), p. 28.

explicitly to 'public radio broadcasts', defined in other parts of the government bill as 'intended for the public', in essence; radio programs.[123] Indeed in the explanation of the relevant section in the preparatory work to the 1966 Radio Act the government explained the relationship of this section to a criminal sanction in the Penal Code of the time dealing with breaking the secrecy of communications. In that context the government concluded that since criminal liability was dependent on the person listening having the *intent* to breach the confidentiality of the communication in question, an individual inadvertently receiving such signals on their radio would not risk committing a crime.[124]

In this light it becomes clear that the Radio Act was not intended to create any wide-ranging exception from the secrecy of communications. The only intent was to secure the right for anyone to listen to public radio programs with a receiver without needing a license. It did not however preclude criminal liability if the individual used a radio receiver to intentionally intercept private communications. It is clear however that the principle has been given a more extensive interpretation over time. Regardless of the logic of such an interpretation, the question is if this principle can maintain a claim of validity in light of more recent legal requirements stemming from EU-law.

5.2 Enter from above: The EU ePrivacy Directive

EU-law enters into this equation through a simple point of fact. By using a mobile phone, an individual is not using a radio transmitter equivalent of a 'walkie-talkie' - openly broadcasting signals to anyone choosing to listen. Though mobile phones contain radio transmitters, the legal implications of the signals they transmit are wider than that. Their use implies also the transmission of messages in an electronic communication system.[125] As such,

[123] Ibid, notably at this time the publicly owned 'Swedish Radio' had a monopoly for such broadcasts, meaning that implicitly radio programs refer to scheduled programming by this company.
[124] Ibid p. 38.
[125] According to article 2 of the Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) "electronic communications network" means transmission systems and, where applicable, switching or routing equipment and other resources which permit the conveyance of signals by wire, by radio, by optical or by other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including Internet) and mobile terrestrial

the communication is covered by the Swedish 'Electronic Communications Act' and the associated protection of communicated data.[126] This act implements into Swedish law the EU ePrivacy directive,[127] which is intended to secure the confidentiality of electronic communication and protect the privacy of those communicating. Accordingly, Ch. 6, Sec. 17 of the Electronic Communications Act prohibits unauthorized access to communications content or associated metadata unless one of the parties to the communication has consented, or if access is allowed by the rules on traditional communications interception.[128] As mentioned above,[129] the use of IMSI-catchers by the Swedish police does not however rely on these rules on interception, indeed the use of IMSI-catchers allow police to bypass normal interception routines and requirements in relation to metadata.

This would – read on its own – mean that the use of IMSI-catchers would be unlawful and subject to criminal sanctions in accordance with the liability rules in the act.[130] However, the prohibition of unauthorized access to communications in the Electronic Communications Act is subject to an exception in Ch. 7, Sec. 6, subsection 3, stating:

> *[The prohibition against unauthorized access] does not preclude using a radio receiver to intercept or otherwise by using such a receiver gain access to an electronic message conveyed by radio, not intended for the person listening or for the public.*[131]

This rule is, according to the preparatory works of the act an expression of the previously mentioned principle that the 'ether is free'.[132] The exception thus precludes criminal liability for unauthorized access of communication taking place over the air. Such

networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed. This definition also applies to the Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector. It is also relevant for Swedish law through its implementation in chapter 1 section 7 of the Electronic Communications Act (2003:389) ('Lag om elektronisk kommunikation') containting a similar definition.

[126] Electronic Communications Act (2003:389) ('Lag om elektronisk kommunikation')

[127] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector.

[128] Chapter 6, section 17 of the Electronic Communications Act.

[129] See section 4.3 above.

[130] Chapter 7, section 15 of the Electronic Communications Act.

[131] Chapter 6, section 17, subsection 3 of the Electronic Communications Act.

[132] Government bill (2002/03:110) 'Lag om elektronisk kommunikation m.m.', (Swedish government 2003), p. 396.

communication is instead left with only a secondary protection in the act through a rule that prohibits, on penalty of a fine, the *disclosure* of information that has been intercepted through a radio receiver and that was not intended for the interceptor, or the public.[133] In other words; it is ok to listen, but if you talk about what you have heard, you will have to pay.

This exception is surprising considering the ePrivacy directive which Ch. 17, Sec. 17 of the act is supposed to implement. In Sec. 21 of the recitals of the directive the need to protect unauthorized access, including access to 'any data related to such communications', is explicitly stated as a purpose of the directive:

> *Measures should be taken to prevent unauthorised access to communications in order to protect the confidentiality of communications, including both the contents and any data related to such communications, by means of public communications networks and publicly available electronic communications services. National legislation in some Member States only prohibits intentional unauthorised access to communications.*

Furthermore, article 5 of the directive, which the Swedish rules on unauthorized access in the Electronic Communications Act is supposed to implement, includes no reference to any principle acknowledging that 'the ether is free'. On the contrary, article 5 states:

> *In particular, [member states] shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorised to do so in accordance with Article 15(1).*

The explicit exception of certain types of unauthorized interception of communication in the Swedish legislation thus seem to be at odds with both the intent and the wording of the directive. Although the Electronic Communications Act prohibits further disclosure of the intercepted information, the directive requires member states to prohibit *access*, not secondary disclosure. Furthermore, the directive specifically covers the use of technical equipment to intercept content as well as and metadata, regardless of the means of communication.[134] Though the ePrivacy directive through recital 11 does not preclude national rules of lawful interception of communication, it is explicit in requiring that any such

[133] Chapter 7, section 15 of the Electronic Communications Act.
[134] In the Swedish language version of the directive, the word 'tapping' in article 5 is expressed as 'uppfångande med tekniskt hjälpmedel' a direct translation of the Swedish version would however be 'interception through a technical device'.

measure must be proportional and in accordance with the requirements of such access under the ECHR as interpreted by the ECtHR. Furthermore, the possibility of authorizing such *exceptions* should not be confused with the scope of protection required by the directive.

5.3 The ether might not be so free after all

All in all, there seems to be several difficulties in applying the principle of 'the ether is free' to IMSI-catchers. The IMSI-catchers used by the Swedish police seem to be of the active variety judging by the information provided by the official report from 2011.[135] As such these are no passive radio receivers which simply gains access to signals in the air. They essentially constitute, as they are described in technical literature, a 'man in the middle attack' on mobile devices within their range, sending signals identifying the IMSI-catcher as a legitimate mobile base-station.[136] By doing so, they depart from the scenario intended to be covered by the legislative exceptions to confidentiality in the Electronic Communications Act, while approaching the scope of the penal code section on the unlawful breach of computer systems. Furthermore, the exception in the Electronic Communications Act relating to radio interception seems to be, at the very least, a doubtful implementation of the E-privacy directive. Considering that the Swedish rules has to be interpreted in accordance with the directive, in order to fulfill the aims of that directive,[137] IMSI-catchers cannot reasonably be allowed to be exempt from the prohibition on interception.

Lastly, while not the focus of this article, it could be argued that by failing to include electronic communication taking place by radio in the protected area of the Electronic Communications Act, the government has essentially undermined the effective protection of private life and correspondence. This may put the Swedish legislation at odds with the positive obligations of the state under the ECHR. These obligations include, but is not limited to, providing an effective protection in law of the rights under the convention. As such, this

[135] See above, section 4.2.
[136] See above, section 2.2.
[137] Cf. for example, *Von Colson* (Case 14/83).

goes beyond limiting interferences attributable to the state, and may include a responsibility to criminalize actions by other private actors that violate the rights of the individual.[138] By excepting radio communications from the protected sphere under domestic law, the state has not only put the individual at risk of unregulated surveillance by state authorities, but essentially opens up for interception by any private person or entity choosing with access to interception equipment. In this context it is worth noting that IMSI-catchers are readily available for purchase on the Internet for a relatively low cost.[139]

5.4 Legality through internal regulation?

As has been developed above, the ether might in fact not be as free as the Swedish legislator lets on. At least not in relation to the confidentiality of communications. For the sake of argument, one might entertain the idea that the principle is valid and the ether (at least in Swedish law) is free. Would this make the Swedish IMSI-catching 'in accordance with the law' as required by article 8(2)? Not likely. The principle of the free ether neither confers powers through substantive law, nor does it limit government discretion; it only serves to create a general exemption of certain pathways of communication from protection from government (and private) interception. As such, it fails to meet the quality of law requirements as articulated by the ECtHR and described in chapter 3 above.

A remaining question is however whether the internal regulation of the police authority may constitute a sufficient basis for the use of IMSI-catchers.

As has been developed in chapter 3 above, the ECtHR has delivered several relevant judgments, with the overall conclusion that while certain aspects of surveillance may be regulated through internal rules or guidelines, certain conditions must be met. Thus, the scope of the powers and discretion given to authorities that serve to limit a right must be accessible,

[138] Cf. *Söderman v. Sweden*, no. 5786/08 [GC], 12 November 2013; *X and Y v. The Netherlands*, no. 8978/80, 26 March 1985, where the failure of the state to secure criminal accountability for violations of privacy was held as a violation of art. 8 of the ECHR.
[139] Alibaba, 'IMSI-catcher' (*Alibaba.com*) <http://www.alibaba.com/product-detail/IMSI-catcher_135958750.html> accessed 27 April 2016

the internal rules need to be legally binding, and the rules must be precise as to minimize discretion and provide foreseeability.[140]

Applying these requirements on the internal regulation of 2011, we see that the regulation is found lacking in several respects. Primarily, the regulation is unpublished and only available through a freedom of information request which in turn is dependent on a prior knowledge of what to ask for. The fact that this request was initially denied with reference to confidentiality, highlights the obscurity of these rules to the general public. Furthermore, the internal regulation contains a general exception allowing derogations from the regulation to be made through a decision by the person in charge of a preliminary criminal investigation, seriously undermining the binding character of the regulation in such cases.

6 CONCLUDING OBSERVATIONS

It is clear that the direct and unmediated nature of IMSI-catchers increases the obscurity of the method, as law enforcement agencies can apply the method without outside assistance. This may also serve to incentivize further obscurity, as any challenges to the legality of its use will be dependent on outside knowledge of such use. Given the Swedish lawmakers apparent hesitance to explicitly legitimize the use of the method through substantive law despite several official reports suggesting this, the Swedish police seem to have responded by enacting its own internal guidelines. As this article shows, this has done little, if anything, to ensure compliance with the ECHR. Meanwhile, the principle of 'the ether is free' has given authorities a manner of legal plausible deniability as it has in practice made certain communication pathways exempt from privacy protections under Swedish law. This principle is likely to have delayed the implementation of a specific legal mandate for the use of IMSI-catchers. The principle of the free ether cannot however survive scrutiny under European law. In fact, the exceptions to the normative privacy protections it has resulted in might, in and of themselves, be regarded as a violation of article 8 of the ECHR and Swedish

[140] See chapter 3 above.

responsibilities under EU-law. That references to the principle has allowed Swedish authorities to apply IMSI-catchers in a manner which must be seen as contrary to article 8 of the ECHR only serves to further illustrate the problematic nature of this principle.

Given that two separate inquiries over a number of years have pointed to the need for a solid legal basis for IMSI-catcher use, the recalcitrance of the Swedish legislator must reasonably be attributed to an unwillingness to surround this method with more stringent safeguards. The requirements of legality in the ECtHR case-law are not new, neither is the appreciation of the problems the principle of the free ether implies. As early as 1992, a Swedish government report highlighted that the principle would likely have to be abandoned as the amount of communication worthy of protection using radio signals was increasing, and as there was low foreseeability for individuals regarding the pathways their communications would use.[141] Given how several legislative initiatives relating to surveillance requiring the assistance by service providers have been taken since the first report mentioning IMSI-catchers, one might reasonably question the delay with regards to IMSI-catchers. One explanation, mentioned in the beginning of this article, is the fact that a legal basis is not, in the case of IMSI-catchers, needed to force private companies to facilitate surveillance.

Beyond the issues relating to the domestic legal basis for IMSI-catcher surveillance this article highlights other concerns. The potential of IMSI-catchers illustrates the need for the ECtHR to develop its case-law on metadata and geo-positional surveillance. Previous cases like *Malone* and *Uzun* have dealt with individual instances of surveillance, and in the case of *Uzun,* surveillance in public spaces. IMSI-catcher use, as developed in section 2.3 above, has more far-reaching implications that need to be addressed. The ECtHR has not yet explicitly recognized the full potential of metadata in mapping the habits and interests of an individual, nor the implications of its use against public gatherings or sensitive locations. Recognizing, like the ECJ has done in *Digital Rights Ireland*[142] and *Schrems*,[143] the implicit sensitivity and

[141] Swedish Government Official Reports (SOU 1992:110) 'Information och den nya Informations Teknologin', (Swedish Government 2010), p. 433.
[142] *Digital Rights Ireland and Seitlinger and Others* (cases C-293/12 and C-594/12, 8 April 2014)
[143] *Schrems* (case C-362/14) [GC], 6 October 2015.

potential of metadata is crucial to secure an effective protection of privacy in the modern communications environment. Granted, IMSI-catchers may be implemented in a way that is substantially less expansive in its privacy implications than the massive surveillance regimes the ECJ has had reason to analyze so far. But, as IMSI-catchers are likely to become more capable, cheaper and more portable with time, the frequency and effect of their use by law-enforcement agencies is likely to increase, and the privacy implications will increase in tandem. Applying rule of law standards similar to those applicable to content would be an important step toward a more solid protection of privacy in this context. In the mean time the Swedish government could do well to live up to its present obligations under ECHR and EU-law by ensuring a substantive legal basis for IMSI-catcher use and the abandonment of the notion that the ether is free.

Acknowledgements

The author would like to thank Johan Lindholm, Therese Enarsson, Lena Landström – all at Umeå University, who read and commented on earlier drafts of this article. This article is a result of the project ’Policing in Sweden – Efficiency and Rule of Law in Police Work’, the funding for which has generously been provided by Riksbankens Jubileumsfond (The Swedish Foundation for Humanities and Social Sciences), grant no. SGO14-1173:1.

TABLE OF REFERENCES

Literature

Alibaba, 'IMSI-catcher' (*Alibaba.com*) <http://www.alibaba.com/product-detail/IMSI-catcher_135958750.html> accessed 27 April 2016

Barrett D, 'Americans' Cellphones targeted in secret U.S. Spy program' *Wall Street Journal* (14 November 2014) <http://www.wsj.com/articles/americans-cellphones-targeted-in-secret-u-s-spy-program-1415917533> accessed 27 January 2016

Bryant B, 'VICE news investigation finds signs of secret phone surveillance across London' (*Vice News*, 14 January 2016) <https://news.vice.com/article/vice-news-investigation-finds-signs-of-secret-phone-surveillance-across-london> accessed 27 January 2016

Bull T, 'Judges without a court : judicial preview in Sweden', *The legal protection of human rights - sceptical essays* (Oxford university press 2011) 392–409

DeNardis L, *The global war for Internet governance* (Yale University Press 2014)

Desmedt Y, 'Man-in-the-Middle Attack' in Henk C. A. van Tilborg and Sushil Jajodia (eds) (Springer US 2011) 759–759

Dirac PAM, 'Is there an Æther?' (1951) 168(4282) Nature <http://dx.doi.org/10.1038/168906a0> 906–907

Einstein A, 'Ether and the Theory of Relativity' in Michel Janssen and others (eds) (Springer Netherlands 2007) 1537–1542

E-mail from author to Registrar, Polismyndigheten (7 May 2015)

Foss AB, 'Slik overvåker norske myndigheter mobiler i Norge' *Aftenposten* (26 January 2016) <http://www.aftenposten.no/nyheter/iriks/Overvaket-mobilaktivitetene-til-egne-borgere-i-flere-enn-35-ulike-tidsperioder-i-fjor-8331223.html> accessed 25 February 2016

Foss AB, Johansen A, and Hager-Thoresen F, 'Secret surveillance of Norway's leaders detected' (*Aftenposten*, 16 December 2014) <http://www.aftenposten.no/nyheter/iriks/Secret-surveillance-of-Norways-leaders-detected-7825278.html> accessed 27 January 2016

Freeze C, 'Guilty pleas end risk of revealing RCMP surveillance technology' (*The Globe and Mail*, 31 March 2016) <http://www.theglobeandmail.com/news/national/guilty-pleas-scuttle-hearing-that-risked-revealing-rcmp-surveillance-technology/article29430116/> accessed 31 March 2016

Fuller LL, *The morality of law.* (2nd edn, Yale University Press 1969)

Government bill (1966:149) 'Förslag till radiolag', (Swedish Government 1966)

Government bill (1975/76:209) 'Om ändring i regeringsformen', (Swedish Government 1976)

Government bill (1992/93:200) 'Om en telelag och en förändrad verksamhetsform för Televerket, m.m.', (Swedish Government 1993)

Government bill (2006/07:63) 'En anpassad försvarsunderrättelseverksamhet', (Swedish government 2007)

Government bill (2006/07:66) 'Angrepp mot informationssystem', (Swedish government 2007)

Government bill (2010/11:46) 'Lagring av trafikuppgifter för brottsbekämpande ändamål – genomförande av direktiv 2006/24/EG', (Swedish government 2010)

Heath B, 'U.S. Marshals secretly tracked 6, 000 cellphones' *USA Today* (23 February 2016) <http://www.usatoday.com/story/news/2016/02/23/us-marshals-service-cellphone-stingray/80785616/> accessed 25 February 2016

Heath B, '200 imprisoned based on illegal cellphone tracking, review finds' *USA Today* (31 March 2016) <http://www.usatoday.com/story/news/2016/03/31/200-imprisoned-based-illegal-cellphone-tracking-review-finds/82489300/> accessed 1 April 2016

Hirschl R, 'The Nordic counternarrative: Democracy, human development, and judicial review' (2011) 9(2) International Journal of Constitutional Law 449–469

Hosein G and Palow CW, 'Modern safeguards for modern surveillance: An analysis of innovations in communications surveillance techniques' (2013) 74 Ohio State Law Journal 1071

Hovmark J and Jacobsson F, 'Marknadsundersökning avseende hemlig teleavlyssning m.m.' (NetLight 2005)

Johansen A, Foss AB, and Hager-Thoresen F, 'New report: Clear signs of mobile surveillance in Oslo, despite denial from police security service' (*Aftenposten*, 26 June 2015) <http://www.aftenposten.no/nyheter/iriks/New-report-Clear-signs-of-mobile-surveillance-in-Oslo_-despite-denial-from-Police-Security-Service-8071885.html> accessed 27 January 2016

Johnson K, 'NSA spying revelations ‘a shock’ to patriot act author' *USA Today* (4 February 2014) <http://www.usatoday.com/story/news/politics/2014/02/04/nsa-surveillance-patriot-act-revelations/5203005/> accessed 29 January 2016

Jonsson Cornell A (ed), *Komparativ konstitutionell rätt* (2nd edn, Iustus, Uppsala 2015)

Koien GM, 'An introduction to access security in UMTS' (2004) 11(1) IEEE Wireless Communications 8–18

Meyer U and Wetzel S, 'A man-in-the-middle attack on UMTS' (ACM Workshop on Wireless Security (WiSe))

Naarttijärvi M, *För din och andras säkerhet : konstitutionella proportionalitetskrav och Säkerhetspolisens preventiva tvångsmedel* (Diss. Umeå : Umeå universitet, 2013, Iustus ; 2013)

Pell SK and Soghoian C, 'Your secret stingray's no secret anymore: The vanishing government monopoly over cell phone surveillance and its impact on national security and consumer privacy' (2014) 28(1) Harvard Journal of Law & Technology

Police authority decision ('Myndighetsbeslut'), Swedish Police Authority, July 3, 2015 (dnr A281.788/2015)

Preliminary decision ('Tjänstemannabeslut') Swedish Police Authority, June 24, 2015 (dnr A194.873/2015)

Reed C, *Making laws for cyberspace* (Oxford University Press 2012)

Sensenbrenner J, 'This abuse of the patriot act must end' *The Guardian* (31 December 2015) <http://www.theguardian.com/commentisfree/2013/jun/09/abuse-patriot-act-must-end> accessed 29 January 2016

Stingray I/II – the secret surveillance catalogue', (*The Intercept*) <https://theintercept.com/surveillance-catalogue/stingray-iii/> accessed 27 January 2016

Swedish Government Official Reports, 'SOU 2010:103 - Särskilda spaningsmetoder, betänkande av Polismetodutredningen' (Swedish Government 2010)

Swedish Government Official Reports ’SOU 2005:38 – Tillgång till elektronisk kommunikation i brottsutredningar m.m., betänkande av Beredningen för rättsväsendets utveckling', (Swedish Government 2005)

Swedish government official reports (SOU 2012:44) Hemliga tvångsmedel mot allvarliga brott, (Swedish government 2012)

Swedish Government Official Reports, SOU 1992:110 – Information och den nya informationsteknologin, betänkande av Datastraffrättsutredningen', (Allmänna förlaget 1992)

United States Department of Justice, 'Policy Guidance: Use of Cell-Site Simulator Technology' (3 September 2015) <https://perma.cc/K99L-H643> accessed 1 April 2016

Řezník T, Horáková B, and Szturc R, 'Advanced methods of cell phone localization for crisis and emergency management applications' (2015) 8(4) International Journal of Digital Earth 259–272

NJA 2007 s. 1037 [2007] Swedish Supreme Court

State of Maryland v. Kerron Andrews [2016] Maryland Court of Special Appeals 1496,

TjF 2011:5 409 - Tjänsteföreskrift om vissa tekniska spaningsmetoder 2011

Örstadius K, 'Misstänkt spioneri mot regeringen' *Dagens nyheter* (18 December 2014)

Case law of the European Court of Human Rights

Amann v. Switzerland, no. 27798/95 [GC], 16 February 2000

Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria, no. 62540/00, 28 June 2007

Bosphorus Hava Yolları Turizm ve Ticaret Anonum Şirketi (Bosphorus Airways) v. Ireland, no. 45036/98 [GC], 30 June 2005

Bykov v. Russia, no. 4378/02, 10 March 2009

Friedl v. Austria, no. 15225/89, January 1995, Series A no. 305-B

Huvig v. France, no. 11105/84, 24 April 1990

Kahn v. The United Kingdom no. 35394/97, 12 May 2000

Kopp v. Switzerland, no. 23224/94, 25 March 1998

Leander v. Sweden, no. 9248/81, 26 March 1987

Malone v. The United Kingdom (8691/79) August 2, 1984

Matthews v. The United Kingdom, no. 24833/94 [GC], 18 February 1999

Peck v. The United Kingdom, no. 44647/98, 28 January 2003

P.G. and J.H. v. The United Kingdom no. 44787/98, 25 September 2001

Roman Zakharov v. Russia, no. 47143/06, 4 December 2015

Silver and others v. The United Kingdom, no. 5947/72; 6205/73; 7052/75; 7061/75; 7107/75; 7113/75; 7136/75, 25 March 1983

Sunday Times *v. The United Kingdom*, no. 6538/74, 26 April 1979

Szabó and Vizzy v. Hungary, no. 37138/14, 12 January 2016

Söderman v. Sweden, no. 5786/08 [GC], 12 November 2013

Taylor-Sabori v. The United Kingdom, no. 47114/94, 22 October 2002

Uzun v. Germany, no. 35623, 2 August 2010

Weber and Saravia v. Germany, no. 54934/00, 29 June 2006

X and Y v. The Netherlands, no. 8978/80, 26 March 1985

Case law of European Union courts

Maximillian Schrems v Data Protection Commissioner (case C-362/14) [GC], 6 October 2015, ECLI:EU:C:2015:650

Digital Rights Ireland Ltd (C-293/12) v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung (C-594/12) and Others (joined cases C-293/12 and C-594/12) [GC], 8 April 2014, ECLI:EU:C:2014:238

Sabine von Colson and Elisabeth Kamann v Land Nordrhein-Westfalen, (Case 14/83), 10 April 1984, ECLI:EU:C:1984:153