Chapter 111
A Paradigm Shift in Swedish Electronic Surveillance Law

Mark Klamberg
Stockholm University, Sweden

ABSTRACT

Electronic surveillance law is subject to a paradigm shift where traditional principles are reconsidered and the notion of privacy has to be reconstructed. This paradigm shift is the result of four major changes in our society with regard to: technology, perceptions of threats, interpretation of human rights and ownership over telecommunications. The above-mentioned changes have created a need to reform both the tools of electronic surveillance and domestic legislation. Surveillance that was previously kept secret with reference to National Security is now subject to public debate, including Communications Intelligence (COMINT), a sub-category of Signals Intelligence (SIGINT). This chapter covers systems of "mass surveillance," such as data retention and COMINT, and whether these are consistent with the European Convention on Human Rights. The chapter comes to two conclusions in relation to COMINT. First, the perceived threats have changed, shifting the focus of COMINT from military threats towards non-state actors such as terrorists and criminal networks. Second, COMINT involves relatively narrow interception of the content of messages compared to its large-scale collection and storage of traffic data, which through further processing may reveal who is communicating with whom.

1. INTRODUCTION

Electronic surveillance is an important tool for law enforcement. Video cameras, wire-tapping, and bugs can be used to detect, prevent, and investigate criminality. It can also be used to collect intelligence about foreign powers or agents of foreign power, which shows that electronic surveillance is not necessarily connected to law enforcement.

Electronic surveillance law is subject to a paradigm shift where traditional principles are reconsidered and the notion of privacy has to be reconstructed. This paradigm shift is the result of four major changes in our society with regard to (1) technology, (2) perceptions of threats, (3) interpretation of human rights, and (4) ownership over telecommunications.

First, the technological development has made the Internet an increasingly important part of our lives. Furthermore, messages are to lesser extent travelling by satellite, microwave relay link and more in fibre optic cable. It is estimated that 95

DOI: 10.4018/978-1-4666-6433-3.ch111

percent of all international communication goes through cable. While satellite and microwave relay links are leaking communication making these modes of communication relatively accessible with an antenna, interception of communication in a fibre optic cable is more problematic. Normally, the cable has to be accessed with the knowledge and consent of the Communications Service Provider (CSP) at certain points where the communication is routed (SOU 2011:13, p. 41; Johnson, 2009; Richelson, 2009).

Second, with the fall of the Berlin Wall and the dissolution of the Soviet Bloc the perceived threats have changed, shifting the focus from military threats towards non-state actors such as terrorists and criminal networks. There is a trend that countries redefine their view of national security, which involves an expanded conceptualization of security. This has led to a shift towards more proactive, preventive measures against threats such as terrorism, in other words preemptive intelligence. A large number of measures involving interference with privacy has been taken to counter such threats (Flyghed, 2005; Omand, 2009; SOU 2011:13, p. 41).

Third, constitutional courts as well as human rights courts have clarified the standards that state agencies have to meet in order to conduct surveillance. For example, article 8 of the European Convention for the protection of Human Rights requires that any individual measure of surveillance has to comply with strict conditions and procedures set out in statute law.

Finally, many European states have towards the end of the 20th century privatized previously state-owned CSPs. In the previous era of state monopolies the State could through secret decrees order their CSPs to hand over communication. Private CSPs are less willing to do the same without a statute creating such an obligation.

The abovementioned changes have created a need to reform both the tools of electronic surveillance and domestic legislation. Surveillance that was previously kept secret is now subject to public debate. There is also a fear that tools created for legitimate purposes such as crime control can also be used for increased or total social control. Does the ends justify the means?

Even if the state does not aim at total social control and the actual surveillance is legitimate, the mere possibility of mass surveillance may lead to self-censorship and inhibition. The option for legislators who do not wish to close down several surveillance systems is to proceed by making the legislation transparent. Some may argue that this would fatally erode the necessary secrecy that need to surround such activity. It is also argued that some of the once-overriding reasons for secrecy have lost their original force while others still remain valid (Solove, 2006; Omand, 2009).

I will first discuss the privacy discourse and provide the essential insights in the electronic surveillance law in Sweden. Methods of surveillance which do not concern electronic communication, such as secret camera surveillance and the use of covert listening devices (bug), is outside the scope of this study. The main focus of the chapter is the signals intelligence operations of the Swedish National Defence Radio Establishment (Försvarets Radioanstalt or FRA). This study is founded on the assumption that FRAs interception of the content of messages is relatively narrow compared to its large-scale collection and storage of traffic data, which through further processing may reveal who is communicating with whom. Does this assumption have any basis in the actual legislation and what consequence will it have for our perception of privacy?