Available online at www.sciencedirect.com
ScienceDirect
Telecommunications Policy 31 (2007) 45–67
TELECOMMUNICATIONS POLICY
www.elsevierbusinessandmanagement.com/locate/telpol

Interceptability of telecommunications: Is US and Dutch law prepared for the future?☆

Bert-Jaap Koops[a], Rudi Bekkers[b,c,*]

[a]*Tilburg Institute for Law, Technology, and Society, Tilburg University, P.O. Box 90153, NL-5000 LE Tilburg, The Netherlands*
[b]*Eindhoven Centre for Innovation Studies (ECIS), Technische Universiteit Eindhoven, P.O. Box 513, NL-5600 BM Eindhoven, The Netherlands*
[c]*Dialogic Innovatie and Interactie, Wilhelminapark 20, NL-3581 ND Utrecht, The Netherlands*

Abstract

For many decades, governments have successfully intercepted telecommunications to collect information about—potential—criminals and terrorists. A crucial part of contemporary policy is legislation that requires telecommunications providers to make their networks and services interceptable. This paper discusses two examples of interceptability legislation: the Communications Assistance for Law Enforcement Act (CALEA) in the US and the Telecommunications Act in the Netherlands, in order to focus on basic questions, considerations, and trade-offs relevant to designing legal interceptability laws.

In particular, the sustainability of interceptability policies as laid down in these laws is questioned, since they are under significant pressure. Technical and market developments challenge their effectiveness and costs. These developments include IP-based services, seamless roaming, default encryption at various telecommunications layers, and the 'identity boom'. Market challenges include substantial shifts in the value chain and the explosion of traffic volumes. This paper aims to determine which interceptability policy is best suited for coping with the challenges that lie ahead.

Keywords: Interceptability; Telecommunications; United States; Netherlands

1. Introduction

Interception of telecommunications is one of the most vital methods for governments to collect information about—potential—criminals and terrorists. In the course of the twentieth century, it became an investigative power that government agencies regard as indispensable, and it is, particularly in some European countries, by far the most widely used special investigation power.[1]

☆*Note*: This article is part of a research project of the first author, funded by the Netherlands Council for Scientific Research (NWO), on law, technology, and shifting power relations. The article is partly based on an evaluation study commissioned by the Dutch Ministry for Economic Affairs on the Dutch interceptability legislation, Koops et al. (2005), and builds on the findings of Arno Smits in his Tilburg dissertation (Smits, 2006).

*Corresponding author. Tel.: +31 40 2475621.
E-mail address: r.n.a.bekkers@tm.tue.nl (R. Bekkers).

[1]See *infra*, Section 3.

0308-5961/$ - see front matter © 2006 Elsevier Ltd. All rights reserved.
doi:10.1016/j.telpol.2006.11.006

Historically, wiretapping[2] has been easy. You plug in to the right telephone line, and you can immediately listen in on the communications. In the 1990s, however, with several changes in telecommunications taking place, including liberalization, privatization and developments in technology and markets, governments were forced to pass legislation in order to make sure that they would continue to have the ability to wiretap. The US Communications Assistance for Law Enforcement Act (CALEA) of 1994 and Chapter 13 of the Dutch Telecommunications Act of 1998, for example, imposed obligations on telecommunications carriers[3] to ensure interceptability.

'Interceptability' means that telecommunications can be intercepted technically on the telecommunications networks or services that transport the communications (technical interceptability).[4] It also includes the ability of telecommunications providers to deliver traffic data[5] or user data, since these may be necessary before a wiretap can be ordered. Interceptability thus means, in short, the ability to investigate telecommunications.

Interceptability legislation is a classic example of the trade-off between public and private interests: obligations—including financial ones—are imposed on private parties, in order to safeguard a public interest. The interest of the private parties—the telecommunications providers—to develop and maintain telecom networks and services as they and the market see fit clashes with the public interest of government agencies who desire to intercept telecommunications and therefore require interceptability. The scope of the obligations imposed within this trade-off, and particularly their financial consequences, which differ from country to country, make this a particularly sensitive and politically heated topic.

This is an appropriate occasion to take a fresh look at interceptability laws. Most of these date from the mid-1990s, an era in which the internet was only just emerging on a larger scale and in which liberalization was only just starting in Europe. Since then, significant developments have taken place in telecommunications, both in the technology and in the market, and these developments continue steadily—for instance with Fiber to the Home (FttH) and Voice over IP (VoIP)—to put pressure on the interceptability of telecommunications. These developments are such that it must be questioned whether the fixation of governments on a sweeping ability to wiretap, as entrenched in legislation, can be continued at all, and if it can, what the costs would be—both financially and in terms of immaterial costs such as privacy and other forms of legal protection.

In light of this, the following questions are posed in this article: How do developments in telecommunications challenge the future interceptability of telecommunications, and how can governments respond to these challenges? Can a balance be maintained between, on the one hand, the ability to counter crime and terrorism through interception and, on the other, the protection against overintrusive government interference?

These questions shall be answered by looking at two countries, the United States and the Netherlands. The former is chosen because the US enacted one of the earliest, if not the first, interceptability laws, and because it has an interesting set of provisions that make the law rather flexible to including or excluding new telecommunications. The second is chosen as a representative of a European legal system that provides an interesting counterexample to the US law. The Dutch law is less elaborate and seems more rigid, with an all-or-nothing approach to new telecommunications; it turns out to be broader in scope than the US law. The Netherlands is also interesting for inclusion because very few publications cover it, so that this article provides the opportunity of opening up the Dutch law to an international audience.[6]

[2]In this article, the terms 'wiretapping' and 'interception of telecommunications' will be used interchangeably. In the US, a distinction is usually made between wire, electronic, and oral interception, following the distinction made in criminal-procedure law; the term wiretapping in this article includes the US wire and electronic interception, but excludes oral interception (which roughly means direct interception, with a bug or directional microphone, of voice communication).

[3]In this article, the terms 'carrier', 'operator', and 'provider' will be used interchangeably for someone who operates telecommunications networks and/or services.

[4]'Interceptability' also includes the obligation that telecommunications carriers comply with legal orders to intercept or to provide traffic data or user data (organisational interceptability). Since this aspect is less vulnerable to developments in telecommunications, this article will be confined to technical interceptability.

[5]Besides interception of telecommunications, which means the content of these communications, governments also have powers to access 'traffic data': data about the communications, such as who called whom when (and perhaps where). In the US, the methods to request access to traffic data are called pen registers and trap-and-trace devices; the term 'traffic-data collection' will be used here.

[6]Academic literature in English is often limited to a comparison between US and UK Law, see for instance Yeates (2001) and Sutter (2001). A comparative description of the interceptability laws in the G7 countries is available in German, see Büllingen and Hillebrand