Chapter II
Intrusion in the Sphere of Personal Communications

Judith Rauhofer
University of Central Lancashire, UK

ABSTRACT

In this chapter the limits for the sphere of personal communications are set. Different understandings of the "right to be alone" or "the right to respect for private and family life" are provided. The significance of the information privacy is pointed out and the right to informational self-determination is deciphered. Having presented the substrate for personal data protection, a legal synopsis of the aforementioned subject is the concluding part of the chapter, with emphasis on data retention.

INTRODUCTION

Sophisticated information technology systems now permeate almost every aspect of modern life. At the same time, there is a threat – whether actual or perceived – that terrorism and organized crime pose to democratic systems of government. This has opened an area of tension between the fundamental right of individuals to respect for their private life and the interest of the state in the protection of its citizens from harm. Modern communications systems, in particular, are seen by many as both, a force for good and bad in the conflict between those who use those systems in the planning and commission of criminal offences and those whose role it is to investigate, prosecute and, ultimately, prevent the commission of such offences by gaining access to the information transmitted and generated by those systems. Historically, the efforts of law enforcement have concentrated on the interception (through wiretapping or otherwise) of communications by suspected individuals with a focus on the contents of those communications. Such surveillance measures were seen by the governments and courts of most democratic countries as restrict-

ing a number of basic human and civil rights, so that, consequently, their use was permitted only in limited circumstances and subject to judicial control and oversight.

With the increased use of electronic communication, however, the focus of law enforcement has shifted to information collateral to those communications, such as the time they where sent, the place from which they were sent and the person or persons to whom they were addressed. This data, which is generated as a matter of course by modern communications systems, not only allows the relevant agencies to track individual suspects but also, it is argued, to trace networks of criminals and to draw conclusions in relation to the methods they use and the level of organization they employ. Access to such collateral data is generally not seen as quite as intrusive as the interception of communications so that a lower threshold would apply when deciding whether or not such intrusions restrict individuals' fundamental rights. However, that data, where it is retained for a longer period of time, inevitably allows those with access to it to build a profile of the individuals to whom it relates, of their actions and their beliefs. Indeed, profiling is now seen as one of the most important weapons in the armory of public and private organizations. It is not only used for the purpose of criminal investigations, but also in the context of a range of other decision-making processes, including, among others, border controls, fraud prevention and financial risk assessment.

Its "human rights relevance" as well as its socioeconomic effect is therefore likely to be much higher than law enforcement agencies will have us believe, and it is both necessary and appropriate to examine these issues at a time when the increased storage and use of such collateral information is being introduced by governments the world over. This chapter will provide a brief historical overview of the legal protection of the right to privacy in Western jurisdictions with particular focus on the concept of "information privacy" and the development of specific data protection legislation in Europe. It will then examine recent legal developments at EU level, including the adoption of the Directive on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC[1] (Data Retention Directive), which requires EU Member States to introduce legislation necessitating the blanket retention of communications data for specified periods. The chapter will look at the way the Directive has been implemented in Denmark, Germany and the UK and the level of harmonization that has so far been achieved. It will then provide an outlook of the consequences, some of them unintended, of blanket retention both in a human rights and in a socioeconomic context.

PRIVACY

Although most Western jurisdictions now protect individuals' rights to control the use and disclosure of their personal information, those rules are based on different origins and, in many cases, different understandings of why such protection is necessary or justified.

The "Right to be Let Alone"

In the US, the right to privacy can be traced back to the famous essay by Warren and Brandeis, which defined privacy as the "right to be let alone" (Warren and Brandeis 1890)[2]. This right, they argued, included the right to control the "communication of [the individual's] thoughts, sentiments, and emotions to others" (Warren and Brandeis, p.198), be they in expressed form (for example, a letter or a drawing) or a mere reproduction by a third party of words or sentiments expressed or actions carried out "in private". Warren and Brandeis claimed that the right to privacy could