Chapter 9
Law and Technology:
Anonymity and Right to Anonymity in a Connected World

Giusella Finocchiaro
University of Bologna, Italy

Claire Vishik
Intel Corporation, UK

ABSTRACT

In this chapter the authors analyze the concept and definitions of anonymity in the modern connected world. In particular, they explore if modern technology renders complete anonymity impossible and if a new definition of anonymity needs to be adopted. They examine examples of anonymous use of technology that illustrate the complexity of the concept of anonymity and demonstrate that access to anonymity is not uniform for data owners with regard to multiple data controllers and audiences in complex systems and processes. They evaluate legal definitions of "anonymity" and "anonymous data" as well as the right to anonymity provided in the European directives and by some European statutes, observing that anonymity cannot be absolute, that only "relative" anonymity is realistic in the present technological environment, and that different degrees of anonymity exist. They address the issue of measuring these degrees or levels of anonymity in complex systems, in order to provide a new foundation for a nuanced and comprehensive understanding of anonymity. The authors conclude that the concept of relative anonymity can become the basis for a new and more effective approach to personal data protection.

INTRODUCTION

Ubiquitous connectivity today makes it easier for the users of systems and networks to find and use information and increase the efficiency and reach of their activities with digitized processes. But in this environment, it is also possible to track users and devices, frequently in order to ensure the fundamental functionality of protocols that is not connected to tracking. Convergent networks and interoperable integrated systems ensure that a record of transactions is available (although not necessarily stored) in a variety of places and can be more easily aggregated and analyzed. An increasing number of transactions, processes, and assets are digitized, leading to greater efficiency in all areas of life and

DOI: 10.4018/978-1-61520-769-5.ch009

organizational operations. We now use electronic data to keep track of our friends' birthdays and send cards to family and friends, to file taxes, to check on pension accounts, to shop, pay bills, and communicate with friends and members of communities of interest. This environment makes our activities more efficient, but it also makes it harder to preserve the anonymity of a user. In an extreme example, it is possible to make an anonymous cash contribution to a charity without any disclosures if allowed by law. But it is not possible to make a truly anonymous contribution to the same charity online, as several data controllers along the path of a transaction – the ISP, the credit card company-- will know (and have the right to know) the identity of the user

As a result, there is an increased interest in the problem of anonymity addressing both technical and legal implications of the new technological environment. From the legal point of view, the main questions are:

- What does "anonymity" mean today?
- Should "anonymity" be considered relative or absolute?
- Does the right to anonymity exist?

From the technical point of view, we can ask:

- What are the technical means to support the highest possible level of anonymity in the modern computing environment without jeopardizing security?
- Can levels of anonymity be measured in an objective fashion in dynamic computing frameworks?
- Does the existence of different "levels" of anonymity available along the path of a message via different systems and networks represent an issue that needs to be remedied? Or is it a normal outcome of the adoption of modern technologies?

TODAY'S COMPLEX COMPUTING ENVIRONMENT

Modern computing environment is characterized by ubiquitous connectivity with ever increasing interoperability among heterogeneous networks and diverse systems and devices. Increasingly, these devices can connect to networks or other devices using a variety of communications protocols: a PC may be using an Ethernet connection as well as connecting over Wi-Fi or WiMax, with Bluetooth, infrared, and 3G options also available. A mobile handset can use modern cellular phone networks and gateways to connect to TCP/IP networks, and also Bluetooth and infrared interfaces. Some GPS devices permit connectivity via Wi-Fi and can act as mobile phones and MP3 players while also connecting to satellites using appropriate protocols. The list can be continued.

Ubiquitous interoperability and connectivity affect computer systems as well as networks. An email application on a mobile phone may use a different client to access the email server, but the data are harmonized when accessed from different devices, and the user can switch to a PC to continue his email or chat communication. An online banking request submitted from a smart phone flows seamlessly through a variety of applications, networks, and gateways, with each component able to recognize the content of the request and authenticate its user and its origin. These transactions always leave an electronic trail that is frequently not captured unless necessary for troubleshooting, non-repudiation support, or other activities. However, some information is always stored for longer periods of time. Typically, only user facing components are analyzed for privacy support, but back-end data exchanged between organizations can also contain sensitive information important to safeguard the users' privacy. Like user-originated data, back-end data contain a number of heterogeneous identifiers.

The move to open standards and federation of standards and services as well as the growing