

# Foreword

Securing privacy in the current environment is one of the grand challenges of today's democracies. While privacy is recognized as a fundamental right of individuals, and the right to privacy is enshrined in laws and constitutions, never before has privacy come under such serious, if not fatal, attacks as in the last few years. This is the result of two broad developments. First, technology is now available (and is routinely used) to entice, collect, store, analyze, and correlate massive quantities of personal data about individuals. The widespread adoption of cloud services and advances in big data techniques from commercial companies have enabled a series of new compelling and useful services (e.g., recommendation services, social networking, targeted advertisement, smart metering), but, at the same time, they have also made possible intrusions into individuals' private sphere on a massive scale. Second, privacy can be abused to hide illegal or threatening behaviors (for example, terrorism attacks). When faced with the choice of security or privacy, governments have increasingly chosen to forego privacy; in fact, as Snowden's revelations have shown, they have obtained broader permissions to engage in large-scale surveillance, in which privacy limitations are eroded in the name of national security.

This Brief in Cybersecurity explores the issues of privacy and security, and their complicated interplay, from a legal and a technical point of view. More precisely, Sophie Stalla-Bourdillon's chapter gives a thorough account of the legal underpinnings of the European approach to privacy, and examines their implementation through the privacy law, data protection law, and data retention law. In particular, it highlights where and how privacy protection breaks down to give way to other (conflicting) concerns, primarily that of security. The chapter by Joshua Philips and Mark D. Ryan focuses instead on the technological aspects of privacy and, in particular, on today's attacks on privacy, determined both by the simple use of today's technology, like web services and e-payment technologies, and by State-level surveillance activities. It also proposes "verifiable surveillance" (a way to make surveillance infringements of privacy quantifiable and verifiable) as a way to reconcile, by technical means, the need of a modern society to both defend privacy and allow well-defined breaches of privacy rights (e.g., for investigations).

It is interesting to observe that the challenges identified by these two chapters suggest that technology and legal instruments in isolation may not be sufficient to protect and put appropriate limits to privacy: technology and legal discourse need one another to draw reasonable lines and erect effective barriers around privacy. We hope this Brief provides a valuable step in this direction.

Marco Cova

<http://www.springer.com/978-1-4471-6529-3>

Privacy vs. Security

Stalla-Bourdillon, S.; Phillips, J.; Ryan, M.D.

2014, VIII, 115 p. 7 illus., Softcover

ISBN: 978-1-4471-6529-3