SPRINGER BRIEFS IN CYBERSECURITY

Sophie Stalla-Bourdillon
Joshua Phillips
Mark D. Ryan

Privacy vs. Security

Springer

SPRINGER BRIEFS IN CYBERSECURITY

Sophie Stalla-Bourdillon
Joshua Phillips
Mark D. Ryan

Privacy vs. Security

Springer

SpringerBriefs in Cybersecurity

Cybersecurity is a difficult and complex field. The technical, political and legal questions surrounding it are complicated, often stretching a spectrum of diverse technologies, varying legal bodies, different political ideas and responsibilities. Cybersecurity is intrinsically interdisciplinary, and most activities in one field immediately affect the others. Technologies and techniques, strategies and tactics, motives and ideologies, rules and laws, institutions and industries, power and money—all of these topics have a role to play in cybersecurity, and all of these are tightly interwoven.

The SpringerBriefs in Cybersecurity series is comprised of two types of briefs: topic- and country-specific briefs. Topic-specific briefs strive to provide a comprehensive coverage of the whole range of topics surrounding cybersecurity, combining whenever possible legal, ethical, social, political and technical issues. Authors with diverse backgrounds explain their motivation, their mindset, and their approach to the topic, to illuminate its theoretical foundations, the practical nuts and bolts and its past, present and future. Country-specific briefs cover national perceptions and strategies, with officials and national authorities explaining the background, the leading thoughts and interests behind the official statements, to foster a more informed international dialogue.

More information about this series at http://www.springer.com/series/10634

Sophie Stalla-Bourdillon · Joshua Phillips
Mark D. Ryan

Privacy vs. Security

Springer

Sophie Stalla-Bourdillon
Southampton Law School
University of Southampton
Southampton
UK

Joshua Phillips
Mark D. Ryan
School of Computer Science
University of Birmingham
Birmingham
UK

ISSN 2193-973X
ISBN 978-1-4471-6529-3
DOI 10.1007/978-1-4471-6530-9

ISSN 2193-9748 (electronic)
ISBN 978-1-4471-6530-9 (eBook)

Library of Congress Control Number: 2014943500

Springer London Heidelberg New York Dordrecht

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

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

Contents

1 Privacy Versus Security… Are We Done Yet? 1
Sophie Stalla-Bourdillon
1.1 Introduction 2
1.2 Privacy Law 6
1.2.1 The Right to Be Let Alone 6
1.2.2 The Right to Respect for Private Life. 8
1.3 Privacy and Data Protection 36
1.3.1 General Data Protection Law 38
1.3.2 Processing by the Police. 50
1.3.3 Processing by Providers of Electronic Communications Services 55
1.4 Privacy and Data Retention 59
1.5 Privacy and Security. 65
1.5.1 National Security, Public Security and the Prevention of Crimes 65
1.5.2 National Security, Public Security, the Prevention of Crimes and Cybersecurity 70
1.5.3 Balancing Privacy and Security 72
1.5.4 Scrutinising Surveillance Measures 76
1.6 Conclusion 86
References 87

2 A Future for Privacy 91
Joshua Phillips and Mark D. Ryan
2.1 Introduction: Privacy Concerns 91
2.1.1 The Problem 92
2.1.2 Overview of Chapter 93
2.2 Taxonomy of Privacy Threats. 94
2.2.1 Big Brother (Governments) 94
2.2.2 Middle Brother (Corporations). 96
2.2.3 Little Brother (Individual People) 96

2.3 Perception and Examples 97
2.3.1 Current Perceptions 97
2.3.2 Examples 98
2.3.3 Content and Metadata. 106
2.4 The Future 107
2.4.1 Our Vision 107
2.4.2 Achieving Privacy, Security, and Accountability 107
2.4.3 Example: Wireless Tickets 109
References 112

Chapter 1
Privacy Versus Security… Are We Done Yet?

Sophie Stalla-Bourdillon

> *"So, we're done. Welcome to a world where Google knows exactly what sort of porn you all like, and more about your interests than your spouse does. Welcome to a world where your cell phone company knows exactly where you are all the time. Welcome to the end of private conversations, because increasingly your conversations are conducted by e-mail, text, or social networking sites.*
> *And welcome to a world where all of this, and everything else that you do or is done on a computer, is saved, correlated, studied, passed around from company to company without your knowledge or consent; and where the government accesses it at will without a warrant".*
>
> —Bruce Schneier CNN March 16, 2013 (Bruce Schneier, The Internet is a surveillance state, March 16, 2013, available at http://edition.cnn.com/2013/03/16/opinion/schneier-internet-surveillance.)

Abstract It is often assumed that privacy and security are alternative values, which cannot be pursued together. Hence, the strength of the "nothing-to-hide argument": if you have nothing to hide, you have nothing to fear. Besides, ensuring the security of the network itself is said to actually require a detailed analysis of network flows. Reasonable expectations of privacy should thus progressively disappear in cyberspace. While it is true that enforcement of legal rules is a real challenge when communications are transmitted through the means of a borderless network, the evolution of the case law of the European Court of Human Right recently followed by the Court of Justice of the European Union does show that the right to respect for private life should have important implications online and in particular should significantly restrict the systematic collection and retention of content and traffic data by both public and private actors such as Internet service providers. At a time at which data-gathering and data-matching technologies are more sophisticated than ever, as illustrated by Snowden's revelations, it is crucial to fully comprehend the interaction between the protection of privacy and the furtherance of security in order to set appropriate limits to surveillance practices. The purpose of this chapter is therefore twofold: first, to shed light upon the European

S. Stalla-Bourdillon et al., *Privacy vs. Security*, SpringerBriefs in Cybersecurity,
DOI 10.1007/978-1-4471-6530-9_1

approach to privacy and explain the interplay between privacy law, data protection law and data retention law; second, to explain how the values of privacy and security should be balanced together and in particular how privacy law should serve to scrutinise the appropriateness of measures implemented to ensure the security of the social group at large.

1.1 Introduction

One of my friends came home on a Sunday afternoon at about 3 p.m. While parking in a supposedly nice and quiet neighbourhood, two cars were waiting behind him for he was blocking the traffic. When he finished his parallel parking, the two cars stopped a few metres further. Something had happened while they were waiting behind my friend's car, but my friend could not really tell what. This is when the driver of the first car went out of his with a baseball bat and in a fury run to the second car and began to beat the car, the front glass, the back glass and then opened the door and continued to beat inside the car. The driver of the second car survived but ended up in hospital with very severe physical injuries. My friend was the only witness. He had called the police who arrived a few minutes after the leaving of the first car. My friend was able to give them the number on the license plate. He was then asked to give a statement to the police. This was the first time my friend had ever witnessed such violence and he was thus really concerned about the possible revenge of the assaulter. Besides, he learned afterwards that the assaulter was a recidivist. He was therefore willing to give a statement to the police as long as his name was not communicated to the defence. Yet, this was not an option available. "Do not worry" said the police officer, "even if we give your name to the defence they will not get your personal details and your address. They will not know who you are. And if you have to appear before a court we will put you behind curtains". And this is what he thought. "I have an unusual name. If the police give my name to the defence the accused will have no difficulty finding me through the means of the Internet. In fact he will have no difficulty finding where I live, where I work and how I look like. If for any reason he decides to take revenge and go after me nothing will stop him".

My friend was thus caught in a dilemma: to render the streets of the neighbourhood more secure radical measures had to be taken against the accused. And this would require him to give a statement to the police and eventually to appear in court. Yet by giving a statement he was agreeing to communicate his name to the defence, which would have had the consequence of putting him in danger, for the accused would then be able to locate him and his family very easily.

What this example shows is at least three things, if not four. First, it demonstrates that in some cases, not to say in many cases, privacy is a concern but not so much in the sense of being able to live or stay in a secluded place away from the public's eyes. What worries people is the subsequent use or misuse of personal information including personal information publicly available. Yet to prevent misuse of personal data, the most efficient way is to minimise the amount of data collected in the first place.