Chapter IV
Protecting Identity without Comprising Privacy:
Privacy Implications of Identity Protection

Ioannis Iglezakis
Aristotle University of Thessaloniki, Greece

ABSTRACT

In this chapter, a specific issue is addressed that concerns the protection of privacy vis-à-vis the efforts to combat identity theft and protect personal identifying information. There are, in particular, measures undertaken by legislators that involve penal sanctions and the introduction of new technological means for identity verification. Also, identity management schemes are introduced, which are utilized by service providers, mainly in the e-business sector, in order to support controlled access to resources. The solutions undertaken to protect identity are seen as measures enhancing privacy, which is endangered by identity theft. Personal information is largely available in the information society and its collection by identity fraudsters is also possible. Therefore, an effective protection of information protection should also include the protection of identity. The downside of the identity protection approach is that identity management actually presents risks to privacy, since the processing of personal data takes place in this context and it is argued that there are certain implications concerning the lawfulness of the processing. The use of electronic authentication through electronic cards or biometrics on passports and identity cards pose privacy issues, too. Subsequently, the legislation concerning identity theft and identity related crime is outlined. This is followed by specific analysis of privacy issues concerning identity management and identity verification methods, with particular reference to biometrics.

Copyright © 2009, IGI Global, distributing in print or electronic forms without written permission of IGI Global is prohibited.

INTRODUCTION

The protection of identity is considered essential today for the reason that identity theft is becoming a serious issue in modern society. As this problem reaches the level of alarm, studies are being carried out which focus on the motives and methods of Internet based identity theft (Marshall & Tompsett, 2005), on the typology of identity related crime (Koops & Leens, 2006) and, what is more important, on the feasibility of measures aiming at combating identity related crime (Halpern, 2006). The said studies stress out expressly that identity theft and identity fraud, which is a broader term, are seen as forthcoming threats, which can jeopardize the interests of users of Internet.

The issue of identity theft is arising due to the availability of information from various online sources. There is a diversity of offered personal information on the Internet, varying from harmless data to more sensitive one, and the collection of information from multiple sources can be used by cybercriminals in order to identity themselves as another person with the intention to commit a financial crime (Marshall & Tompsett, 2005). So, for example, the European Network and Information Security Agency (ENISA) presented recently a Position Paper on Security Issues and Recommendations for Online Social Networks at the e-challenges conference in Hague, in which it outlined the threats to users and providers of such services, e.g. digital dossier aggregation (creation of digital dossiers of personal data), secondary data collection (collection of traffic data), face recognition (user images being used to enable linking to apparently anonymous profiles) etc.[1]

By and large, it seems that the Internet can be used as a medium for the exploitation of identity information, which is available in a wide variety and its acquisition is an easy task, while it is difficult for law enforcement authorities to seek and capture illegal activities. Information and Communication Technologies (ICTs) and the Internet make it possible for anyone to collect personal information through the access of public records. Identity thieves have been able to take on the identity of a victim or even work anonymously in order to access web resources in order to commit fraud (Chawki & Wahab, 2006).

The Internet is, of course, not the only source for obtaining personal information that can lead to identity fraud. Fraudsters seem to be able to find any piece of information relating to an individual and may use various tactics to get it. A recent example is the theft of a laptop in UK, which contained unencrypted information about 600,000 people.[2] Similar incidents have also taken place with regard financial information and the competent authorities have sanctioned financial organizations for their failure to take appropriate measures. The methods of obtaining identity information are either technical or non-technical. The former methods include key logging, (e.g., via malware on user's system), hacking into a legitimate database and collection of data by a counterfeit website (preceded by phishing attacks), whereas the latter include the retrieval of materials from waste bins, social engineering and mail or data theft (Furnell, 2007a, p. 6).

Identity theft is committed by offenders in order to perpetrate fraud, usually by obtaining a financial benefit in someone else's name[3]. In more particular, it has as its object the personal identifying information of another individual, including inter alia name, address, date of birth, phone numbers, utility bills, passport, driving license, birth certificate, bank details and credit card information, employment information, social security number, e-mail address, passwords, etc., and it purports to opening or taking over of credit card accounts, applying for loans, etc (Chawki & Wahab, 2006, p. 3). However, the appropriation of an identity itself will not give rise to criminal offense, unless it is performed with the intention to commit an illicit activity (Savirimuthu & Savirimuthu, 2007, p. 439). Identity fraud is generally related to threats such as phishing and pharming, which are emerging as new forms of fraud committed electronically.

25 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:
www.igi-global.com/chapter/protecting-identity-without-comprising-privacy/29357

Related Content

Legal Provisions for Contracts During Pandemics: A Practical Study on the COVID-19 Pandemic According to UAE Legislation
Fouad Al Shaibi, Abdulla Ali Binmalek, Akmal Ramadan Ramdanand Khulood Eid Abdulaziz (2026). *Digital Evidence and Procedural Law in the UAE (pp. 109-134).*
www.irma-international.org/chapter/legal-provisions-for-contracts-during-pandemics/406893

Latest Trends in Deep Learning Techniques for Image Steganography
Vijay Kumar, Sahil Sharma, Chandan Kumarand Aditya Kumar Sahu (2023). *International Journal of Digital Crime and Forensics (pp. 1-14).*
www.irma-international.org/article/latest-trends-in-deep-learning-techniques-for-image-steganography/318666

On Cloud Data Transaction Security Using Encryption and Intrusion Detection
Mahmoud Jazzar (2020). *Digital Forensics and Forensic Investigations: Breakthroughs in Research and Practice (pp. 17-26).*
www.irma-international.org/chapter/on-cloud-data-transaction-security-using-encryption-and-intrusion-detection/252675

Blockchain Technology Is a Boost to Cyber Security: Block Chain
Sowmiya B.and Poovammal E. (2019). *Countering Cyber Attacks and Preserving the Integrity and Availability of Critical Systems (pp. 254-266).*
www.irma-international.org/chapter/blockchain-technology-is-a-boost-to-cyber-security/222228

Audio Tampering Forensics Based on Representation Learning of ENF Phase Sequence
Chunyan Zeng, Yao Yang, Zhifeng Wang, Shuai Kongand Shixiong Feng (2022). *International Journal of Digital Crime and Forensics (pp. 1-19).*
www.irma-international.org/article/audio-tampering-forensics-based-on-representation-learning-of-enf-phase-sequence/302894