

Chapter VII

Navigating in Internet: Privacy and the “Transparent” Individual

Christina Akrivopoulou

Aristotle University of Thessaloniki, Greece

Aris Stylianou

Aristotle University of Thessaloniki, Greece

ABSTRACT

The chapter faces a series of questions that the digital era raises as far as the protection of privacy is concerned. Technology and specifically internet, apart from posing innovative, complex threats to the autonomy and privacy of the individual constructs a new frame for approaching privacy. The technological texture of the internet calls for a new conception of privacy that can be adopted in those circumstances, such as anonymity. The chapter argues that though anonymity cannot be identified with the right to privacy, represents in fact one of its key functions, its ability as a negative freedom to shield the autonomy of the individual against all kind of threats. Thus, anonymity can foster communication, speech and political expression in the internet. Nevertheless, the cost of protecting privacy as anonymity is substantial since its neutral character can function as a veil for sinister actions such as libel, hate-speech and stalking in cyberspace. The need for ‘reconceptualizing’ privacy in the internet, for the writers confirms the evolving, developing character of the right, whose substantial content is not given or static but is closely connected and constructed via societal change. The chapter explores the technological threats that the right to privacy confronts in the internet, such as “cookies”, “spam messages”, the dangers they pose to the freedom and autonomy of the individual as well as the positive dimensions of the internet, especially its role in democratic accountability and political dialogue. Concluding the writers present three architectures for the protection of privacy in the internet: (a) a model based on informational law, (b) a market based solution, where privacy is understood in contractual terms and (c) a model based on the participation of the users in the uses of their personal information as well as to the enforcement of the accountability of the internet actors, e.g. corporations, advertising agencies.

INTRODUCTION

Why is Internet an Unfriendly Place for Privacy?

Privacy in the internet seems to be a myth for the ordinary user, for four distinct and yet interconnected reasons. First, it's the open character of the internet. The fact that we can log in our mail at any time, from anywhere, raises serious doubts about the confidentiality of our communication. The open character of the internet suggests that anyone can retrieve information from our personal page, our curriculum vitae, or even our photographs and use them for purposes different from those an individual had originally intended to. Secondly, it's the interactive nature of internet. Internet for the most is a part of everyday life; we use it to communicate with our friends, for professional reasons, to be entertained, to be informed or to acquire products, leaving behind us, our traces. With our ability to deny or give our consent, in limiting our privacy, as our only shield, interaction in the internet can pose serious threats to our freedoms. The third reason, for contesting privacy in the internet, is its global dimension. National legislation protecting our personal data seems ineffective since internet has no borders or limitation. In the end, the unique speed, the flow rate of the internet, as well as its ability to process information in a small amount of time, presents new challenges for the protection of our informational privacy, mainly because it enables the formation of our personal profile, by the bits and pieces of information that we are leaving behind as we are websurfing.

This chapter, is attempting to analyze this ambiguous relation between internet and the right to privacy, by posing and approaching a series of questions. In the first part of the chapter, we are facing the problematic of the way that information threatens privacy by examining, (a) the technological texture of the threats that the internet is posing to privacy, (b) the way those threats are affecting

the autonomy and freedom of the individual, through judicial paradigms of Greek courts, as well as of the European Court of Human Rights, (c) the conflict between transparency of information, as a clash augmented by the use of internet and the protection of privacy. In the second part of the chapter, we examine the way a right to privacy can be conceptualized and protected in the internet by examining, (a) the right of privacy as a right constructed by the technological evolution, (b) a concept that privacy adopts in the frame of the internet, as anonymity and (c) the ways privacy can be protected in the frame of internet, through information privacy law, a market based solution, or a balanced architecture which enables control over data internet practices of institutions as well as the participation of the individual in the uses of their information.

THE TECHNOLOGICAL DEVELOPMENT AS A WISH AND AS A CURSE: INFORMATION VS PRIVACY

Internet and Privacy: Old Threats in New Clothes

Internet and the threats that pose to privacy are often dealt as something, emerging as utterly new. Whereas this statement is not completely untrue is quite misleading, since in reality, the threats that internet poses to privacy, are actually familiar: **loss of control over personal information, disclosure of private facts and surveillance of an individual.** All of them are threats connected with the rise of the information age, the first one identified to the use of computer data-bases and the other two to the application of monitoring devices, such as cameras. Nevertheless, these threats are merely intensified and augmented by the use of internet. Internet is threatening privacy as a completely new of course and highly atypical form of data-base (Katsch 1995). It threatens privacy because it can extract information; since

12 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/navigating-internet-privacy-transparent-individual/29360

Related Content

Locally Square Distortion and Batch Steganographic Capacity

Andrew D. Ker (2009). *International Journal of Digital Crime and Forensics* (pp. 29-44).

www.irma-international.org/article/locally-square-distortion-batch-steganographic/1590

Privacy Compliance Requirements in Workflow Environments

Maria N. Koukovini, Eugenia I. Papagiannakopoulou, Georgios V. Lioudakis, Nikolaos L. Dellas, Dimitra I. Kaklamaniand Iakovos S. Venieris (2015). *Handbook of Research on Digital Crime, Cyberspace Security, and Information Assurance* (pp. 157-177).

www.irma-international.org/chapter/privacy-compliance-requirements-in-workflow-environments/115756

Evaluation of Autopsy and Volatility for Cybercrime Investigation: A Forensic Lucid Case Study

Ahmed Almutairi, Behzad Shoarian Satari, Carlos Rivas, Cristian Florin Stanciu, Mozhdeh Yamani, Zahra Zohoorsaadatand Serguei A. Mokhov (2020). *International Journal of Digital Crime and Forensics* (pp. 58-89).

www.irma-international.org/article/evaluation-of-autopsy-and-volatility-for-cybercrime-investigation/240651

Drug Law Enforcement in an Agent-Based Model: Simulating the Disruption to Street-Level Drug Markets

Anne Dray, Lorraine Mazerolle, Pascal Perezand Alison Ritter (2008). *Artificial Crime Analysis Systems: Using Computer Simulations and Geographic Information Systems* (pp. 352-371).

www.irma-international.org/chapter/drug-law-enforcement-agent-based/5272

Criminal Jurisdiction and Modern Technology: A Comparative Study

Abdulghani Al-Shuaibi, Ahmed Aldabousi, Abdalla Alhosani, Fatma Lashkaran Alraeesand Ayman Fekry (2026). *Digital Evidence and Procedural Law in the UAE* (pp. 199-224).

www.irma-international.org/chapter/criminal-jurisdiction-and-modern-technology/406897