Chapter 7.7
Responsibility for Information Assurance and Privacy:
A Problem of Individual Ethics?

Bernd Carsten Stahl
De Montfort University, UK

ABSTRACT

Decisions regarding information assurance and IT security can affect individuals' rights and obligations and thereby acquire a moral quality. The same can be said for questions of privacy. This article starts by showing how and why information assurance and privacy can become problems worthy of ethical consideration. It demonstrates that there is no simple and linear relationship between ethics and information assurance, nor between ethics and privacy. Many decisions in the area of IT, however, affect not only one but both of these subjects. The ethical evaluation of decisions and actions in the area of privacy and security is therefore highly complex. The article explores the question of whether individual responsibility is a useful construct to address ethical issues of this complexity. After introducing a theory of responsibility, the article discusses the conditions that a subject of responsibility is typically assumed to fulfil. The article will argue that individual human beings lack some of the essential preconditions necessary to be ascribed responsibility. Individuals have neither the power, nor the knowledge, nor the intellectual capacities to successfully deal with the ethical challenges in the tension of privacy and information assurance. The article ends by suggesting that the concept of responsibility may nevertheless be useful in this setting, but it would have to be expanded to allow collective entities as subjects.

INTRODUCTION

Proponents of information assurance aim at meeting the security testing, evaluation, and assessment needs of information technology (IT) consumers and producers. They are mostly interested in eliminating security threats and in the long run want to increase the levels of trust that users and consumers have in IT and networks. While most users support these goals of information assurance, they also have other objectives when using IT, among them the preservation of privacy. To a certain degree these two objectives are contradictory. In order to facilitate security,

CBT

it would be helpful to eliminate privacy because this would allow an easier detection and elimination of security risks. Privacy, on the other hand, requires security because the protection of private data relies on the assumption that no unauthorised access is possible. Privacy and information assurance can thus also be complementary.

Further complicating this relationship, both terms also have an ethical side to them. Trust as the ultimate aim of information assurance is a moral notion, at least in some aspects. Security is necessary to facilitate a free and equal exchange of ideas. At the same time an excess of security can stifle the exchange of ideas and thus the greater good. Privacy is generally recognised as morally good, but it is debatable how this good can be justified and where its limits are. The individual user who must make decisions concerning the weighting of privacy and information assurance therefore finds him or herself in a situation where, despite an ethical quality of the choices, it is less than clear how decisions are to be made.

This is where the concept of responsibility enters the picture. This article will describe a theory of responsibility and put a special emphasis on the question of who can be the subject of responsibility. This theory of responsibility will then be applied to the complex problem of privacy and information assurance. The theory and conditions of responsibility will be used to demonstrate that, while individual responsibility can play an important role in such ethical decisions, it also runs into severe problems. It will be argued that due to the lack of fulfillment of the basic conditions of responsibility, the individual end user is not able to shoulder the burdens required in order to make an ethical decision. The end user in this article will be understood to be an individual using IT. The reason for using the term "end user" is that it emphasises the individual aspect, the fact that a human individual is using technology. End users can be private users of technology but also individuals working in organisations. It will be argued that end users as individuals lack some of

the qualities necessary for the successful ascription of responsibility. As a consequence, questions of privacy and information assurance require a wider context and frame in which they can be answered. Only in such a frame does individual responsibility make sense and can it achieve its objectives.

How should the individual end user deal with this dilemma? The conclusion of the article will argue that the content of this article is of high relevance for the individual end user because it allows him or her to recognise the limits of their capacities. The very fact that individual humans quickly reach their fundamental limits when they are ascribed responsibility in the context of information assurance and privacy will allow them to overcome their limitations. By pointing out why they cannot accept such responsibility ascriptions, they should be able to transcend the ascription and open discourses that will include other subjects that, in turn, might be able to solve the problem. Briefly, the arguments presented in the article can be used to protect the individual end user from responsibility ascription, which he or she is incapable of satisfying. At the same time they should help avoid situations where responsibility is wrongly ascribed to individuals.

INFORMATION ASSURANCE & PRIVACY: AN ETHICAL CHALLENGE

As indicated in the introduction, a brief look at the concepts of information assurance and privacy could suggest that the two can be contradictory, but the opposite interpretation is just as possible. Since it is the purpose of this article to analyse the role that individual responsibility can play with regard to the realisation of information assurance and privacy, this section will be dedicated to a discussion and definition of the concepts. In both cases the focus of the discussion will be their ethical content and the ethical challenges they pose.

Related Content

Learning from Patterns During Information Technology Configuration

Keith S. Hortonand Rick G. Dewar (2005). *Journal of Organizational and End User Computing (pp. 26-42).*

www.irma-international.org/article/learning-patterns-during-information-technology/3797

A TAM Analysis of an Alternative High-Security User Authentication Procedure

Merrill Warkentin, Kimberly Davisand Ernst Bekkering (2005). *Advanced Topics in End User Computing, Volume 4 (pp. 280-300).*

www.irma-international.org/chapter/tam-analysis-alternative-high-security/4483

Web Caching System: Improving the Performance of Web-based Information Retrieval System

Sathiyamoorthi V. (2017). *Design Solutions for User-Centric Information Systems (pp. 184-204).*

www.irma-international.org/chapter/web-caching-system/173974

A Survey of Micro-Mainframe Links

Judith D. Ahrensand Samuel D. Strum (1992). *Journal of Microcomputer Systems Management (pp. 1-12).*

www.irma-international.org/article/survey-micro-mainframe-links/55680

An Image-Text Matching Method for Multi-Modal Robots

Ke Zhengand Zhou Li (2024). *Journal of Organizational and End User Computing (pp. 1-21).*

www.irma-international.org/article/an-image-text-matching-method-for-multi-modal-robots/334701