BILETA 2008 Conference
Law Shaping Technology; Technology Shaping the Law
GLASGOW CALEDONIAN UNIVERSITY

Trojans, Agents and Tags: The Next Generation of Investigators

Wiebke Abel
SCRIPT, the AHRC Research Centre for Studies in Intellectual Property and Technology Law, School of Law, University of Edinburgh
Email: w.abel@sms.ed.ac.uk

Abstract

Recent developments in Artificial Intelligence and Computer Science have influenced the way police forces and law enforcement agencies are operating and combating crime. The evolvement of autonomous and semi-autonomous technologies has led to the adoption of new investigating and evidence gathering methods.

This new generation of technologies, such as Trojans, RFID tags and autonomous software agents, features unique abilities which considerably distinguish them from existing technologies currently used in investigations and will allow them to gradually replace human investigators in their designated areas. During investigations, these technologies are able to go beyond the mere execution of operator commands, and act autonomously. Also, compared to existing evidence gathering technologies, such as CCTV, they are invisible to the suspects.

These abilities pose a challenge to existing legislation regulating police investigations and evidence gathering, and the admissibility and interpretation of this evidence in court. The question is in how far existing legislation is still adequate and sufficient to regulate the use of these new technologies in crime investigations.

In attempting this analysis, this paper examines a topical example, the intended use of the "German Federal Trojan" ("Bundestrojaner") by German authorities in criminal investigations.

The German government is planning to introduce (and to some extend has already used) a new investigating method for police forces and secret services, the "German Federal Trojan". According to these plans, it will be possible to remotely search private computers (and laptops) of suspects using a Trojan or some other

similar type of malicious software (malware).[1] This malware will be implanted on the computer without the knowledge of the suspect and will be used to intercept the email traffic and to copy, and subsequently transfer back to the operator, any file stored on the computer that seems relevant to the investigation. The Trojan could either be distributed as an email attachment or by making use of a security hole (so called backdoor) in the operating system.[2] The internet will thereby enable the Trojan to "move" around and also serves as a means to transport the data and communicate with the operator. The Trojan will be able to install itself on the computer and, to at least (semi)autonomously search the stored files and emails on it and make a selection on what data is important and relevant.

In the first part, this paper will examine the technical aspects of the "Federal Trojan" and describe its intended use in criminal investigations. In the second part, an analysis of the challenges the law faces in the light of this technology will occur, thereby examining in how far existing legislation is able to deal with this new form of evidence collection method.

[1] Leipold K., "Die Online-Durchsuchung", NJW-Spezial 2007, 135.
[2] Rux J., "Ausforschung privater Rechner durch die Polizei- und Sicherheitsbehörden", JZ 2007, 286.