ECBA Autumn Conference
Tallinn
October 2, 2012

Digital evidence outside cyber space:
the implications of electronic data in "non-cyber" cases

Jaanus Tehver

LAW OFFICE
Tehver & Partners

What is cybercrime?

- *Offences against the confidentiality, integrity and availability of computer data and systems*
  - *- illegal access to computer systems (hacking, cracking, etc)*
  - *- illegal interception of computer data (monitoring, surveillance recording)*
  - *- data interference (deletion, alteration, input of malicious codes such as viruses, etc)*
  - *- system interference, i.e. hindering function of computer system (sabotage)*
  - *- misuse of devices (programs and other 'hacker tools')*
- *Computer-related offences*
  - *- computer-related forgery*
  - *- computer-related fraud*
- *Content-related offences*
  - *- offences related to child pornography*
- *Offences related to infringements of copyright and related rights*
  - *- infringement of copyright and related rights by means of a computer system*

Convention on Cybercrime (Budapest, 23.11.2001), Ch 1, Section 1

Digital evidence, definition

- Digital evidence is defined as any data stored or transmitted using a computer that supprt of refute a theory of how an offence occurred or that address critical elements of the offence.

(Eoghan Casey, 2011)

Digital evidence in non-cyber cases?

- „Digital evidence is becoming a feature of most criminal cases. Everything is moving in this direction.“

  Susan Brenner, University of Dayton School of Law

  Year: 2005

- „Cyber crime is only a subset of a much broader trend in the criminal area, which is the use of digital evidence in virtually all criminal cases.“

  Thomas K. Clancy, University of Mississippi School of Law

  Year: 2011

Implications for the defence, I

- Effective defence can only be done by lawyers who know how computers work
- Gathering and submission of defence evidence, as well as responding to prosecution evidence, demands computer literacy
- In addition to basic IT knowledge and skills, a fundamental understanding of how digital data is created, handled, presented, and perceived, is vital

Implications for the defence, II

- Defence usually begins from a position of disadvantage, mainly because:

  a) huge volume of information means that different conclusions can be drawn from the same data, depending on what to look for, how and where to look, what to disregard, etc;

  b) prosecution has vastly more resources (time and money) to analyze and report on evidence data;

continues...

Implications for the defence, III

c) since ‘experts’ have been involved in the collection and analysis of evidence, it is commonly believed to be reliable;

d) possibilities to challenge admissibility are limited;

e) defence’s access to ‘original’ data is limited, and challenging the authenticity of copies is difficult.

Implications for the defence, IV

- Most criminal defence practicioners are not adequately trained in IT issues in general, and in ESI and digital evidence and computer forensics in particular.
- Investigators, government experts, prosecutors, and even judges have received much more training in this field.
- To achieve eqality of arms, this will have to change

Implications for the defence, V

- Due to limited resources, defence in cases relying heavily on digital evidence usually employs the tactic of finding loopholes, legal technicalities, etc.
- In order to do this successfully , the defence counsel must be competent in technical as well as legal aspects of digital evidence, and can not depend solely on expert advice.

Implications for the defence, VI

- The interaction between law and rapidly developing technology pushes changes in well-established legal concepts (search and seizure rules, protection of privacy, etc), and as a consequence, lawyers must be familiar with cutting-edge case law and new theories

Implications for the defence, VII

- Due to decreasing reliance on oral evidence (witness statements) at trial, the proceedings have become more difficult to follow from the judge's perspective, and from the defence point of view, it makes it harder to persuasively convey his/her story
- Cross-examination as a well-established means of testing evidence is increasingly unavailable

Implications for the defence, VIII

- Large amounts of various pieces of electronic information means that the prosecution can introduce a lot of irrelevant material as circumstantial evidence to prove his/her story
- Digital evidence often needs to be interpreted by a specialist. Expert's involvement means that judges tend to attribute more weight to such evidence, even if the material is actually irrelevant or unreliable.

Implications for the defence, IX

- Defence arguments challenging the authenticity and integrity of digital evidence are often dismissed as speculation
- The form and style in which digital evidence is presented during pre-trial disclosure and at trial often makes it very difficult for the defence to actually analyze and challenge the data

Implications for the defence, X

- The huge volumes of data, and the complexity of analysis of this data, inevitably means that the cost of effective defence will be very high in growing number of cases
- Increased cost and increased uncertainty of the outcome in cases relying heavily on digital evidence will almost certainly create a situation where defendants are more likely to accept plea bargaining or similar proceedings, and give up fighting for their innocence

Summary, I

- Digital evidence certainly does not make defence work easier for the defendant and the counsel. On the contrary, the challenges caused by the proliferation of digital evidence mean that defence attorneys must acquire completely new skills to survive and properly serve their clients.

Summary, II

„The new defence lawyer must be a technician, able to use software and equipment, but also a sort of film producer, able to present digital evidence in a clear, gripping fashion portraying a persuasive, sensible narrative. The new lawyer must be both engineer and artist. The two roles are so intimately connected that the lawyer cannot sever them.“

Andrew E. Taslitz, Howard University School of Law

Year 2004

Final question

How to make precedent-obsessed,
backward-looking,
math-and-techno-phobic
lawyers
(most of us)
learn the new ways?