Electronic evidence, expertly explored

Crime moves with the times, with the law hard on its heels... Pirates and highwaymen do still exist, but these days they are likely to have smartphones, and the proof needed to catch and convict them is probably digital. With new questions about electronic evidence constantly arising, EU-funded researchers have mapped out a path towards a common framework.

© pict rider - fotolia.com

The EVIDENCE project, which ended in October 2016, was dedicated to the application of new technologies in the collection, use and transmission of electronic evidence. “The aim was to provide the European Commission with a roadmap for harmonisation of the exchange of this type of evidence in the Member States,” says project coordinator Maria Angela Biasiotti of Italy’s Consiglio Nazionale delle Ricerche.

The project has established a dialogue among stakeholders who were not naturally inclined to consult with each other, Biasiotti reports. It also developed a common language for the description and handling of electronic evidence, and produced a catalogue of digital forensic tools in use. Building on these advances, the partners eventually submitted the proposed roadmap for consideration by the European Commission.

Proof on the move

Electronic evidence comes in many forms, including files secured from a hard drive, CCTV footage or content from social media platforms. Harmonised practice would help to make the most of any such material available – to prevent crime, prove a perpetrator’s guilt, or indeed establish a defendant’s innocence.

However, the evidence needed in one country may well originate in another, which may not apply the same rules when it comes to the acquisition, use and transmission of this material. These discrepancies currently complicate its use.

There are many ethical, legal and technical issues to consider, says Biasiotti. For example, she notes, the tools used may vary from one EU country to another. They also tend to be proprietary, and therefore much harder to harmonise than open source versions might be.

And, of course, even within individual EU countries, key stakeholders may disagree on the best way forward. Internet service providers (ISPs) and law enforcement agencies, for example, don't usually see eye to eye when it comes to the disclosure of personal data. Having paved the way for dialogue is one of the project's most notable outcomes, says Biasiotti, who reports that EVIDENCE has fostered the emergence of a European electronic evidence community where all sides are represented.

Exchangeable across the EU

The fight against terrorism is one area where the potential and the complexity of sharing electronic evidence have been thrown into sharp relief. Terrorists commonly use social networking sites to organise attacks, Biasiotti notes. "In this context, it is important for law enforcement agencies to exchange electronic evidence, in order to prevent what is happening," she says.

"This is information stored by an ISP," Biasiotti explains. "It would help to have an agreement with the ISP to provide it without delay, and a way to convince the ISP that the need to investigate outweighs the need to protect the privacy of a particular person."

In addition, she notes, a shared formal language is required to facilitate the exchange of material from different sources and in different languages. "This way," Biasiotti comments, "we can put all the pieces of electronic evidence together, and this combined evidence is described in a way that makes it easier to use for the law enforcement agencies that have to act to prevent crime."

Along with this formal language, EVIDENCE developed a catalogue of tools used to deal with electronic evidence. This inventory lists more than 1 500 programmes and devices, for tasks as varied as acquiring data from a live computer, analysing cloud storage configuration files or investigating messages hidden in images or other files.

The project's roadmap thus draws on advances in several areas. To prepare for its implementation, says Biasiotti, campaigns should be organised to raise awareness at operational level, among those who may be involved in exchanges of such material but may not be fully acquainted with the issues.

And the proposed formal language needs to be tested: the EVIDENCE partners are hoping to secure funding for trials where it would be plugged into the secure data exchange infrastructure developed by e-Codex, another EU-funded project. As always, the proof is in the pudding – or, in this case, in the pilot project.

Project details

- Project acronym: **EVIDENCE**
- Participants: Italy (Coordinator), Netherlands, France, Germany, Malta, Belgium, Bulgaria
- Project N°: 608185
- Total costs: € 2 303 649
- EU contribution: € 1 924 589
- Duration: March 2014 - October 2016

See also

Project website: http://www.evidenceproject.eu/
Project details:
http://cordis.europa.eu/project/rcn/185514_en.html

View the article online:
http://ec.europa.eu/research/infocentre/article_en.cfm?artid=43496