Digital Investigation 25 (2018) 1–4

Contents lists available at ScienceDirect

Digital Investigation

journal homepage: www.elsevier.com/locate/diin

Editorial

Transdisciplinary strategies for digital investigation challenges

Digital investigations have many facets, and one's perspective frames the perception and prioritization of challenges in our field. The following examples of various stakeholders' concerns demonstrates the multitude of issues in digital investigations. Law enforcement personnel perceive procedural challenges, such as gaining timely access to data on encrypted devices or in the cloud. Computer scientists perceive technical challenges, including reverse engineering and big data analysis. Forensic scientists perceive challenges establishing links between virtual and physical entities, and evaluating the probability of evidence given one claim versus a given alternative claim. Criminologists perceive challenges obtaining a global view of crime trends and developing broader strategies for abating crime. Business managers perceive risk management challenges, including data theft and associated regulatory penalties. Psychologists perceive victimology challenges to understand and mitigate vulnerabilities that make certain people more prone to attacks. Intelligence analysts perceive challenges in maintaining national security. Privacy advocates perceive challenges of protecting private information from unauthorized access. The public perceives challenges that they become aware of through the media and personal experiences.

This wide range of challenges emphasizes the need for transdisciplinary problem-solving that balances the various interests and risks. Although digital evidence is being widely used to support decisions in courtrooms, boardrooms and war-rooms, questions are mounting about the reliability of forensic results, and technical and legal barriers are forming to block access to data. Although the digital investigation and forensic communities have made tremendous progress over the past two decades, there are emerging challenges that we must address. There is a strong community of researchers and practitioners working towards finding workable solutions for the benefit of the global society, but groups that pursue their special interests without consideration of other perspectives may create more problems than they solve.

What our field needs now are solutions that balance multiple, often conflicting, interests. The editorial team of this journal brings together multiple viewpoints in order to foster effective transdisciplinary strategies for addressing major challenges in digital investigations.

Access to digital investigation capabilities

First consider the pros and cons of restricting digital investigation capabilities to only those with large amounts of money, power or knowledge.

Digital investigations are becoming more expensive and difficult, making them unattainable for less funded researchers and practitioners, open source tool developers, students, and even developing countries. The impediments are due in part to licenses for proprietary solutions, the use of exploits to access locked-down devices, and advanced techniques like chip off requiring specialized equipment and expertise. The use of strong cryptographic techniques, as well as the rapid development cycles, limit the information that is available for use in digital investigations. Furthermore, manufacturers of digital devices are adding security enhancements that make digital investigations more challenging. For instance, Apple recently announced plans to disable USB access on devices locked for over one week. Such security enhancements fuel the ongoing debate over whether manufacturers should be required to add alternative access methods for lawful use.

One perspective is expressed in “Editorial from my iPhone” (Volume 16, March 2016): it is safer for a democratic government to develop its own closely held techniques for extracting data from locked mobile devices for lawful use rather than compelling manufacturers to compromise security. Others argue that the current model for extracting digital evidence from embedded systems such as mobile devices needs to fundamentally change. Current extraction methods are based on unsystematic hacking and cracking of these devices. Whoever has the best hacks and cracks in their toolbox gets the best evidence. Over time, these vulnerabilities are patched, and the data extraction methods no longer work. This process is too unreliable and introduces risks of destruction or modification of evidence.

Digital investigators do not hack into email accounts to get access to email evidence — a legal request is made to the mail provider. Digital investigators do not hack into websites or cloud environments to get content evidence — a legal request is made to the content hoster. It should also be possible to bring a mobile device to its manufacturer and make a legal request for evidence extraction — no hacking required. Concerns about unauthorized access via alternative access methods are valid and must be addressed. However, such concerns are the same as those relating to unauthorized access via vulnerabilities. In both cases, unauthorized access risks can (and should) be mitigated with software updates when discovered by the manufacturer.

Now consider the opportunities and risks of making digital investigation capabilities more freely available, including law enforcement officers at a crime scene, security personnel in a company, authoritarian regimes, individual hackers, organized

https://doi.org/10.1016/j.diin.2018.05.002

criminals, protective parents, and suspicious spouses. Depending on the context and use, digital investigation capabilities can be used as beneficial tools or harmful instruments. Digital investigation capabilities are used to maintain a safe society, countering cybercrime and terrorist attacks. On the other hand, individuals who lack proper governance have misused digital investigation capabilities beyond their authorization, thereby violating the law.

These opportunities and risks are compounded by the growing number of always watching, always listening devices spread throughout digitalized society that sense activities and generate associated traces (e.g., smart assistants, smart glasses, pervasive CCTV, smart car cameras). In some cases, only digital witnesses remain. However, the same data sources could be used to oppress dissenting views.

There is no simple remedy for these complex challenges. Designating government sponsored entities to administer digital investigation capabilities can concentrate investment of new solutions, and reduce illegal misuse, but is not globally equitable. Governments with more resources to invest in exploiting vulnerabilities and extracting data have a digital investigation advantage which can lead to large power imbalance. Developing countries have limited resources to conduct digital investigations, limiting their ability to combat corruption and violence, which could contribute to political and economic instability. Furthermore, even highly secure centralized control is not failsafe. To support digital investigations, the U.S. government developed new ways to exploit vulnerabilities in Microsoft operating systems, but the information was stolen and subsequently used in illegal attacks, including the WannaCry epidemic in 2017.

Reliability concerns of digital investigation results

The stakes are high in digital investigations, often impacting a person's livelihood or liberty. Therefore, it is crucial to avoid mistakes, missed opportunities, misinterpretations, and miscarriages of justice.

An ongoing challenge in digital investigations is ensuring the reliability of evidence produced by non-specialists in various contexts. In the UK, problems with the use of digital investigation capabilities by law enforcement led the Forensic Regulator's 2017 report to express the concern that "*if quality of forensic science provision is of insufficient priority to enable risks to be managed effectively and quality standards to be achieved, the logical result is that it will become unsustainable for any forensic services to be managed within some police forces.*"

To improve the quality and reliability of forensic results, best practice guides are being developed and maintained by ENFSI and SGWDE. In addition, standards from ISO and ASTM are being promulgated to establish quality assurance and reliability of forensic results.

An added challenge is that telemetry data collected by service providers is already being used in forensic investigations, but the reliability is not always well established. For instance, when a digital investigation is concerned with location using cell site analysis or geolocation information from mobile devices, it is important to take into account possible errors. In addition, digital investigators must evaluate and express their forensic findings as outlined in "Clearly conveying digital forensic results" (Volume 24, March 2018).

Another challenge is assessing the reliability of results produced by various forms of artificial intelligence that are being applied to analyzing data gathered during digital investigations. For instance, machine learning can produce reliable results but experts often have difficulty explaining how the results were obtained. This issue is further compounded when feature extraction and correlation are performed entirely by algorithms using deep learning analysis techniques. Cloud providers offer easy access to multimedia analysis services based on black box, pre-trained models for a range of use cases from object identification to human characteristic estimation (e.g., age, height, gender, etc.). Should we simply trust the machines?

As expressed in Peter Sommer's commentary in the present issue "Accrediting digital forensics: What are the choices?" there is no panacea, and a mixed solution is needed.

Balancing digital investigations with privacy concerns

In addition to extracting data from individual devices, governments and industry are gathering massive amounts of information from computers and communication systems to gain profound insights into peoples' activities and behavior, creating opportunities for digital investigations and posing substantial privacy risks. In Ireland, a homicide investigation that led to the conviction of Graham Dwyer relied heavily on telecommunications data to correlate the movements of personal and anonymous burner mobile phones over time. In a growing number of crimes, people taking videos with their mobile devices have provided valuable digital evidence. In the future, a crowd of people with smart glasses might be used as a collective evidence source.

Advanced analysis of large amounts of data can improve understanding of the crime and the criminal, enabling a more focused investigation such as where to find additional evidence, what deserves deeper inspection, and even where to avoid spending time and effort. The growing amount of information that is being collected in digital investigations can also be used to obtain a broader understanding of crime, criminals, victims and vulnerabilities. Combining information from multiple offenses can link crimes committed by the same offender(s), can detect trends in criminal activities, and can help develop more effective investigative and preventative strategies.

On the other hand, organizations with sufficient money, power or knowledge can exploit these data sources, utilizing big data analysis to target individuals with a specific agenda (e.g., Cambridge Analytica). In addition, criminals are gaining unauthorized access to massive amounts of sensitive information (e.g., Equifax).

Within Europe, the General Data Protection Regulation (GDPR – EU, 2016/679) is attempting to find a balance between the risks and the possibilities for law enforcement. However, these legislative changes could create challenges for digital investigations. Notably, Graham Dwyer is appealing his conviction, arguing that the collection of evidence in his case violated his privacy rights.

By 25 May 2018, the GDPR must be implemented into the local laws of EU member states. Many companies have adapted their business processes to comply with these new laws to avoid costly penalties for non-compliance. It is expected that many of these developments will result in less possibilities to collect information from companies, although the many exemptions might give opportunities for governments.

Digital privacy plays a central role in modern society. Digital investigations help resolve data breaches and misuses of personal information. Misuses of big data analysis by corporations and governments is corroding public trust in technology. Legislation must simultaneously protect personal data from such misuses, and enable lawful investigations into criminal activities. In addition, streamlined legal processes are needed to help digital investigators combine information from multiple offenses, to tackle international or organized crime and to develop broader strategies against crime.