Digital Investigation 22 (2017) 1–2

Contents lists available at ScienceDirect

Digital Investigation

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

Editorial

The value of forensic preparedness and digital-identification expertise in smart society

Imagine a city awash in data that leak personal information about peoples' lives. Mobile devices scan the airwaves for attractions and deals in the surrounding area, and resulting purchases generate transaction records (e.g., credit cards, peer-to-peer payments, and crypto currencies). Details about citizens' movements and health are beamed out by wearable technology (e.g., activity trackers and geolocation recorders) and implanted medical devices (e.g., pacemakers, defibrillators, and neuro stimulators). Vehicles steer through streets and the sky (e.g., cars, trucks, and drones), recording and reporting details about their environs for navigation and safety. Offices and homes monitor and regulate their access (e.g., cameras, motion sensors, and door locks) and environment (e.g., heat, light, and entertainment devices). Public spaces are under surveillance through an increasing number of smart technologies, including IP CCTV cameras, license plate recognition systems, and police drones.

In actuality, this situation already exists in many cities today. People are allowing their digital traces to flow all over the place, accepting unknown risks in exchange for immediate gratification. With the convenience of these technological advances comes the risk of hacking, government surveillance, and business misuse. Hackers are exploiting these systems to steal valuable or sensitive information, and to launch attacks on the Internet. Corporations are collecting data to sell more products, and sometimes simply sell the data to other corporations. Police are using digital traces to investigate and disrupt criminal activities, and occasionally obtain information they are not authorized to have. In addition to generating data, smart technologies are programmed to perform tasks, sometimes employing artificial intelligence.

Assignment of legal responsibility for decisions that are enabled by smart technology depends on the ability to identify (with sufficient confidence) the entities behind the technology. *"In case of accidents or misbehavior, current laws require that the physical or legal principal behind the entity be found so that she can be held to account. This may be problematic if the linkability of the principal and the operating entity is questionable." (Koops BJ, Hildebrandt M, Jaquet-Chiffelle DO. Bridging the Accountability Gap: Rights for New Entities in the Information Society? Minnesota Journal of Law, Science & Technology. 2010;11(2):497–561).*

Digital investigators have much to learn about smart technologies in order to investigate crime and handle security breaches in this context. This issue has the first in a series of articles that will be published in the Journal of Digital Investigation dealing with challenges created by smart cities from both a digital forensic and cyber-security perspective (Future challenges for smart cities: Cyber-security and digital forensics, by Baig et al.).

Digital investigators also have ample opportunities to apply their digital-identification expertise, thus contributing to the effective use of identity-related information in smart society.

Digital investigation and smart society

Detailed digital traces can paint a vivid picture of a person's daily life. Normal activities in smart society leave a cybertrail that can be used to reconstruct an individual's whereabouts at specific times, including access to his office or home, his electronic purchases, and much more. In some situations, digital traces give us more information than traditional traces such as fingerprints. For instance, in the physical world, it is often unknown when a fingerprint was present, whereas digital traces often capture the date and time when a person's fingerprint is detected. As a result, smart technologies can help answer investigative questions such as when and where a crime occurred, who was involved, exactly what happened, and sometimes why. The same information is used by corporations to inform business decisions. Hackers can misuse this information in imaginative ways to harm victims physically, mentally and financially.

As more decisions in society depend on data and actions from smart technology, the reliability and security of these systems are critical. In a smart society that strives to make intelligent decisions on the basis of reliable information, digital investigators can play a critical role. Digital investigators have experience challenging assumptions, answering questions such as "Does the system actually protect personally identifiable information (PII) or does it actually store this information in a manner that could permit unauthorized access?" Digital investigators also have experience finding irregularities in complex computer systems, answering questions such as "How did the intruders circumvent security measures to gain access to the system?"

It is not just the data from smart technology that must be reliable, but also the analysis of the raw data, as well as the actions and conclusions drawn from them. Digital investigators, in their role as digital-identification experts, use well-established methods and processes from forensic science to address questions and support decisions. These same methods and processes can help improve how data-driven decisions are made in smart society, and not only in a criminal justice context. Many sectors of smart society can be bolstered by digital-identification expertise, including commerce, economy and politics.

http://dx.doi.org/10.1016/j.diin.2017.09.001
1742-2876/

(Un)reliability of big data

Given the volume, variety, velocity and decentralization of data in smart society, it is difficult to verify that specific information is complete and correct. An increasing number of smart technologies are continuously generating data and automating tasks, and little is being done to ensure that these digital traces and algorithms are reliable and secure. The resulting risks are substantial, including identity usurpation resulting in financial losses, false identification leading to arrests, and erroneous credit history undermining loan applications. Technologies that perform tasks on our behalf can be dangerous and even deadly, such as autonomous vehicles crashing after failing to detect obstacles.

Some data scientists believe that data speaks for itself, without the need for independent verification of the reliability of underlying raw data and algorithms. Such faith in technology and big data is foolhardy, ignoring irregularities that occur in every computerized process and system, and which can result in digital traces that are incomplete or erroneous.

If we think of smart technologies as digital witnesses or digital informants, they might not always provide reliable information. As with traditional (human) witnesses and informants, we must take precautions to verify what they tell us.

If we think of digital devices as measuring instruments, they might be inaccurate or incorrect under certain conditions. For example, Assisted GPS (AGPS) geolocation coordinates recorded by a digital device can be inaccurate in some situations. Investigators and forensic scientists deal with errors in measuring instruments at crime scenes and within forensic laboratories. Why should we expect digital devices roaming about in the world to be much different or better?

There are always gaps in the data we collect, which entail uncertainty. After an event involving smart technology has occurred, it can be difficult to verify the reliability of underlying data and automated tasks, particularly when there is a lack of forensic preparedness. Forensic preparation includes maintaining a digital evidence map of critical data sources, and having properly trained personal at the ready to implement response plans and procedures for handling incidents in a way that satisfies legal, privacy and forensic requirements. Without forensic preparedness, we will not have adequate visibility into crimes and attacks in smart society. Even when we find a digital device that might be pertinent to our case, the digital traces are no longer available, or are located in a cloud environment that we cannot access, or are in proprietary formats that we do not know how to interpret. Even if the raw data or audit trail are retained for verification purposes, they are not being retained in a forensically sound manner to ensure their integrity. These same limitations can negatively influence decisions that depend on data, and autonomic activities in business, governance, and other areas of smart society.

Given the potential for error and omissions, we must be careful not to jump to conclusions on the basis of smart technology or big data alone. To support solid decision making, it is necessary to evaluate digital traces, and to correlate information from independent sources. Lessons learned from criminal investigation, and forensic science processes developed over the past 100 years, can help with these challenges in new contexts. This is especially true for identification – the process of establishing "sufficient confidence in the fact that some identity-related information describes a specific entity in a given context, at a certain time" (Casey E, Jaquet-Chiffelle D-O (2017) "Do Identities Matter?" Policing: a Journal of Policy and Practice, Special Issue, Oxford University Press, Available at https://doi.org/10.1093/police/pax034).

Uncertainty in identification

Digital-identification plays a critical function in smart society, and poses significant challenges. Ultimately, it is difficult to establish a link between virtual and physical entities. Although more of our activities leave digital traces in smart society, it can be extremely difficult to link those digital traces to an actual person in the physical world – there is usually some level of uncertainty. For example, voice commands on my Amazon Echo account might give the impression that I was in Baltimore (where my Amazon Echo device is located) at a time when I was actually in Lausanne. In fact, anyone near the Amazon Echo device can speak a command, which is then recorded on my Amazon Echo account. Therefore, it is not safe to assume that activities in my Amazon Echo account relate to me. Additional context is needed to correctly interpret the digital traces and to perform a proper identification.

Given these uncertainties, digital investigators must be cautious when forming identification conclusions on the basis of digital traces. Corporations must also be wary of data that they use to advertise and sell products. How can they be sure that a specific marketing campaign influences a specific customer's behavior?

For over a hundred years, investigators and forensic scientists have been performing identification using traces in the physical world. Many of the same concepts can be applied to smart technology and big data. Digital investigators are in a strong position to provide digital-identification expertise, adapting existing techniques and developing new approaches to identification in smart society.

Conclusions

Society has become heavily dependent on smart technology, creating exciting opportunities and unexpected risks. Digital investigators can help increase the security and reliability of information generated by smart technologies and the tasks they perform. Forensic preparedness can be applied to smart technologies to ensure that data are reliable, just as processes and controls can be put in place to prevent misuse by hackers, police and corporations. In addition, for identification purposes, it is necessary to examine assumptions about the underlying information, and to evaluate the confidence of links between the information and specific entity. *Effective forensic preparedness and digital identification provide a solid foundation for assigning legal responsibility and protecting personal information, including the EU General Data Protection Regulation (GDPR)*, including data privacy and right to erasure ('right to be forgotten') requirements. Digital investigators play a crucial role in smart society, supporting detection and investigation of crimes and attacks. Beyond digital forensics and incident response, they can help provide reliable information and identification to support decisions in many context, including commerce, economy and politics. The opportunities for digital investigators and digital-identification experts in smart society are burgeoning.

Eoghan Casey
Editor-in-Chief
University of Lausanne, Switzerland
E-mail address: eoghan.casey@unil.ch.