Article

Do Identities Matter?

Eoghan Casey* and David-Olivier Jaquet-Chiffelle*

Abstract It is difficult to overstate the importance of identity in the digital age, as well as the importance of digitized information for identity. In order to advance security, liberty, and privacy in modern society, it is crucial to understand the nuances of what identity means and how it is used and abused. This article defines identity, covering both physical and virtual entities, which is relevant in diverse contexts such as forensic science, cybersecurity, and national security. This article concentrates on the relevance of identity in forensic science, and provides illustrative examples. Approaches and challenges to evaluating and expressing confidence in identity-related conclusions are discussed. Privacy issues are considered along with the rising risks of identity usurpation and impersonation. Relationships between identification of physical and virtual entities are addressed, including the weaknesses and strengths of digital information alone, and the benefits of combining multiple forensic disciplines when assessing identity. This article concludes with a consideration of the benefits for forensic science specifically, and society generally, to take a pluridisciplinary approach to establishing identity.

Introduction

> Identity is established by authenticating that information characterizes a specific entity in a given context, during a certain time, with sufficient confidence. Identity establishment (identification) is essentially subjective as it depends on an authenticator's perspective and evaluation.

Forensic science and criminalistics have grown out of the belief that every entity in the universe is unique. The term *individualization* has been used to describe the use of information to identify something to the exclusion of all others (Kirk, 1963; Inman and Rudin, 2002). In practice, individualization of an entity is only feasible within a specific context and time, not universally (Champod and Evett, 2001; Cole, 2009). SWGFAST (Scientific Working Group on Friction Ridge Analysis, Study, and Technology) has struggled with the term individualization (SWGFAST, 2013). To reduce confusion, forensic scientists are clarifying the distinction between individuality and identification, and are eschewing the use of individualization (Robertson *et al.*, 2016; Champod, 2013).

Identification is the decision process of establishing, with sufficient confidence (not absolute certainty), that some identity-related information describes a specific entity in a given context, at a certain time (Jaquet-Chiffelle, 2009).

Identification can have probative value both in the early investigation phase, to help narrow the suspect pool and highlight missing information,

*Ecole des Sciences Criminelles (ESC), Université de Lausanne, Batochime, CH-1015 Lausanne-Dorigny, Switzerland. E-mail: eoghan.casey@unil.ch

Policing, pp. 1–14
doi:10.1093/police/pax034

and in later phases to support decisions in court (Jackson *et al.*, 2006). Decisions in the early investigation phase such as following leads typically require less confidence than the later conclusion phases, particularly in court. The increasing demand for forensic results to be expressed in an unambiguous and transparent manner is motivating more formalization in how conclusions related to identification are evaluated and expressed (Biederman *et al.*, 2016).

The understanding of identity has expanded to encompass the evolution of virtual entities (Jaquet-Chiffelle, 2009). In addition, there is increased understanding that identity can change with the context and time, such as a person's virtual identity, gender identity, or identity being usurped and misused. The term identity usurpation is used instead of identity theft 'since identity is not something that is typically stolen; unlike theft, where the owner loses possession over the stolen good, the victim of identity takeover still retains her identity' (Koops *et al.*, 2009). Taking all of these considerations into account, a clearer definition of identity has been developed, stated above and explained further below.

This article begins with the nuances of identity and how it is used in forensic science, explicates the differences and connections between identities of physical and digital/virtual entities, addresses uncertainty and confidence in identity, and highlights the growing concerns relating to identity, privacy and criminality.

How is identity used?

Identity plays a role in many important functions of daily life in modern society, both in the physical world and cyberspace, including banking, shopping, travelling, and voting. Certain misuses of identity are considered crimes, including identity creation (e.g. fake ID) and identity usurpation (Koops *et al.*, 2009). From a forensic perspective, identity-related information is used to guide investigative decisions and to help judges and juries make decisions of innocence or guilt.

In forensic science, identity has many uses and nuances both in the physical and digital realms. Identity is not limited to people: things (material and digital) and virtual entities also have identities. Methods in forensic science that support identification decisions deal both with full identities that describe distinct entities, physical or virtual, and with partial identities which place entities with certain shared characteristics into a particular class. Another nuance is that forensic science can support conclusions relating to the identity of a person or thing to varying levels of confidence, short of absolute certainty. In a criminal case, it might be necessary for decision makers to be convinced of identity with *extremely high confidence*, whereas in a civil case *strong confidence* might be sufficient, and in a natural disaster *moderate confidence* might be adequate. For instance, taking an individual's fingerprints and comparing them against a database of previously collected information to find potential matches might be sufficient to identify a body in a natural disaster, or even to consider the person as a potential suspect in a criminal investigation.

In certain situations, forensic analysis is used to determine the nature of a trace (e.g. blood stain, cocaine, elephant tusk), i.e. to find information that confirms the class identity of a trace-entity with sufficient confidence. When it is broadly accepted that the used analytical method is discriminant enough, the decision about identity is not necessarily left to the judge or the jury.

In other situations, more circumspection is called for when assessing the strength of the link between a known entity and observed traces, especially when the entity is the suspect—a possible source of the litigious activity that produced the observed traces. In such situations, the results of forensic analysis should be evaluated and expressed in terms of the traces rather than the entity. The final leap of faith is ultimately a

decision for judges and juries, not for forensic experts, as expressed in Jackson *et al.* (2006) (with quotation from Doheny v Adams [1997] 1 Cr.App.R 369):

> 'The scientist should not be asked his opinion on the likelihood that it was the defendant who left the crime stain, nor when giving evidence should he use terminology which may lead the jury to believe that he is expressing such an opinion' The likelihood, or probability, that it was a particular defendant who left a crime stain depends not only on the strength of the scientific evidence but also on the combined strength of the other non-scientific evidence. If a scientist gives a view on the probability of the origin of a crime stain, then that view will be limited by the scientist's inevitably partial knowledge of the totality of the evidence in a case. Potentially misleading opinion could then be given.

When examining a disaster victim, when a body is in bad condition, or when ante-mortem information is sparse (both physical and digital), addressing questions of identity can be difficult (Gremaud, 2010). Some murders attempt to fight forensic analysis by removing identity informative features from their victims. However, it is difficult to subtract all identity-information from a person, including digital traces.

> Case Example (Gaumer, Maryland, 2005): After killing Josie Phyllis Brown, John Gaumer cut-off her fingertips, jawbone, teeth, and nose in an attempt to thwart identification of her body. On the basis of cellular service provider records, investigators refuted Gaumer's claim that he drove her home after their date. Inadvertently, while Gaumer was attacking Brown, his mobile device dialled her phone, resulting in a voicemail recording of the victim pleading for her life and then being beaten to death.
>
> These digital traces of Brown's last movements and exclamations helped investigators persuade Gaumer to bring them to and identify her body (McMenamin, 2006, 2007).

Another challenge is how to identify an unknown offender using traces at a crime scene, such as bite marks, hairs, fingerprints, and biological fluids. Additionally, if the perpetrator carried a mobile device, passed by CCTV systems, or drove through toll booths while engaged in criminal activity, he might have inadvertently generated digital traces through cell towers, surveillance cameras, and other information systems.

> Case Example (Dwyer, Ireland, 2012): Dwyer was convicted of killing Elaine O'Hara, dumping her body in remote woods, and throwing her personal possessions into a reservoir, including a set of keys and the victim's supermarket loyalty card. Forensic examination of the victim's computer and mobile device revealed a likely suspect who was an architect named 'Graham' involved in online forums for bondage-discipline-sadism-masochism (BDSM), and interested in flying model aeroplanes. Graham was careful to only communicate with the victim using phones that were not tied directly to his identity. However, the location of one of these phones and Dwyer's personal phone was determined to be the same over a period of time. On the basis of phone locations at particular times passing through toll gates, photos were

> obtained showing Dwyer's license plate passing through the toll gates. In addition, analysis of semen stains found in the victim's bed provided a DNA profile that was compatible with the profile of Dwyer (Raidió Teilifís Éireann, 2015; Stack, 2015).

The process of finding Graham Dwyer demonstrates the nuances of identity, including the distinction between physical and virtual entities, and the usefulness of characteristics that have high selectivity versus low selectivity as shown in Table 1. In essence, characteristics with high selectivity provide distinctive identity-related information, whereas characteristics with low selectivity only provide information useful for establishing partial identity. In certain circumstances, a physical appearance on CCTV can be highly selective, depending on the clarity and angle of the picture. Similarly, a large quantity of accurate data points tracking an individual's location over a period can be highly selective because a small number of people follow the exact same path for very long.

Characteristics such as those in Table 1 can combine to create a compelling picture of identity as shown in Fig. 1.

What is identity, explicitly?

Before delving into the complexities and challenges associated with identity, it is helpful to explicate what constitutes identity in practical terms.

Characteristics to establish identity

The characteristics that can be useful for establishing identity are varied, and extend into the digital realm (Jaquet-Chiffelle, 2009). In terms of people, such selective characteristics fall into the four categories in Table 2.

The fourth category (something that you do/prefer) is becoming more prevalent in digitized society. A simple example is a behavioural biometric such as keystroke dynamics, which is being used to identify people on the basis of their distinctive typing patterns (Teh *et al.*, 2013). Various digital traces that a human being generates simply by living in the modern world can be combined to establish (partial) identities, effectively creating a behavioural biometric. For example, reconstituting a person's movements over time (between home, work, etc.) on the basis of location data recorded by a smartphone, SatNav device, or automobile can be used to identify the individual to some degree of confidence. Our likes and preferences can lead to patterns such as shopping habits, which could also be part of behavioural biometrics. Some financial institutions verify identity by asking a combination of questions about things you did in the past; accumulation of things you did have been described as biographical identity (Koops *et al.*, 2009).

Not only human beings

In the context of forensic science, any animate or inanimate entity, physical or virtual, can be identified using selective characteristics. Some illustrative examples:

Fauna and flora: when an animal tusk or skin is found in a tourist's luggage, forensic analysis might be able to determine that it came from an endangered species, potentially leading to criminal charges. Some characteristics can be used to determine species, i.e. find the identity of a species, but not the specific animal within a particular species, while other characteristics can help establish the identity of a specific animal in a species (Coquoz and Taroni, 2006). Certain characteristics can be used to relate entities to each other and their approximate location, potentially leading to crime hotspots (Wasser *et al.*, 2015).

Objects: a crime scene typically comprises many traces that can be used to identify objects, including patterns on shoeprints, treads on tiremarks, and striations on bullets. Computers and mobile devices have traces that are used to identify them such as mobile equipment identifiers (e.g. IMEI),

Table 1: Examples of high and low selectivity characteristics of physical and virtual entities

Entity	High-selectivity characteristics	Low-selectivity characteristics
Physical (human being)	• DNA • Face	• Is male • Is named 'Graham Dwyer' • Is doing BDSM • Is working as an architect • Is a model aeroplane enthusiast • Is married with children • Is at location (L) at time(t) • Physical appearance on CCTV
Virtual (entity)	• Secret mobile phone number (086-175-9076) • Mobile phone number (087-210-0407) • Car license plate number (99-G-11850) • Email address (fetishboy@gmail.com)	• 'Architect72' (online pseudonym) • 'Graham' (online pseudonym) • Architect (role) • Member of BDSM community (activity) • Aeroplane enthusiast (interest) • Married with children (status) • Recorded at location (L) at time(t)

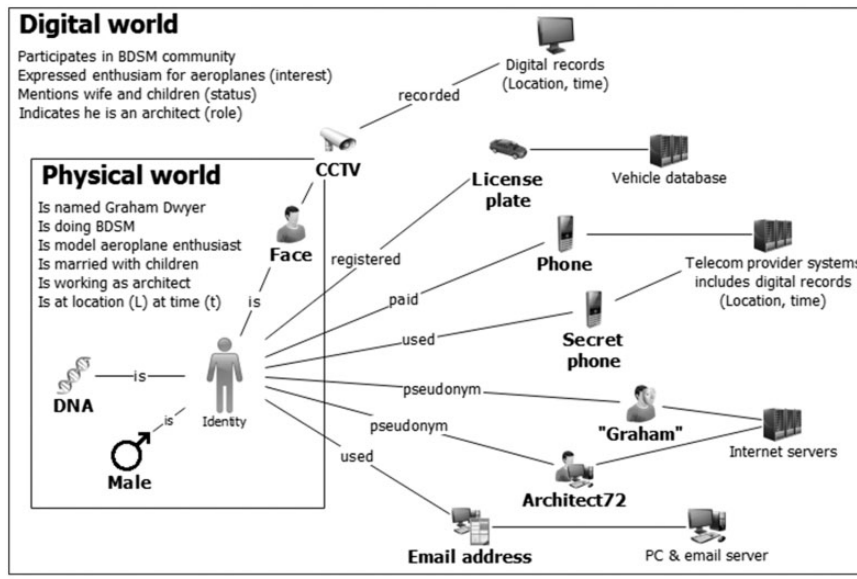

Figure 1: Characteristics of physical and digital/virtual entities combining to form a suspect's identity.

Table 2: Categorization of characteristics that are useful for establishing identity

Something you . . .	Examples
Are	Biometric features such as a fingerprint, voiceprint, retina, or face.
Have	Passport, smartcard or SIM card (phone number)
Know/choose	PIN, password
Do/prefer	Behavioural biometrics or behavior patterns, or biographical identity

subscriber identifiers (IMSI) and advertising identifiers (e.g. IDFA). Some traces can be used to determine the class of an object (class identity, i.e. a partial identity for the objects of this class), and others, which are more distinctive, allow to distinguish a specific object within its class, i.e. to establish its identity.

Locations: some landmarks, background terrain, or other characteristics can be used to determine a particular region, and others can reveal a specific place in that area (Bolton, 2016). Under certain conditions, the approximate location where a digital video was recorded can be identified using electrical network frequency (ENF) analysis (Garg et al., 2013).

Virtual: online activities can be associated with virtual entities, which can complicate identity. A virtual entity (persona) can be used to anonymize online activities, effectively concealing the physical entity (human being) performing the actions. Furthermore, a virtual entity can perform actions without the direct involvement of a human being, e.g. an autonomous system such as a chatbot.

> Case example: The Sweetie 2.0 chatbot was developed to find online sexual predators in video chatrooms. The chatbot presents the face of a young child, and responds to conversation using preprogramed phrases. Even though the chatbot is simplistic in its interactions, this initiative has been successful at finding sexual predators. [http://www.universiteitleiden.nl/en/research/research-projects/law/sweetie-2.0]

Uncertainty and confidence in identity

Identity plays a critical role in many investigations, even when it is partial. For instance, distinguishing between shoeprints made by different kinds of shoes can narrow the suspect pool to those people with a specific make of shoe.

Uncertainty in identity

There is always some gap between identifying information and the actual thing (Robertson *et al.*, 2016). This gap is relatively small for forensic analysis of DNA, with a remote possibility of a suspect's DNA profile being compatible with more than one human being. The challenge of linking identity information to the actual thing is exacerbated when characteristics that comprise identity change over time, or are usurped and misused. Wear patterns on a shoe or tire can change with use over time. Striations that a gun makes on a bullet can change with use over time. Landmarks at a location can be added or removed. An online persona (a particular virtual person) can be used by a different person in the future. Some companies reassign a telephone number to a new customer after some period of disuse by the previous customer. Even the characteristics that are closely coupled with a person (something you are) can change with age, and can be digitized and falsified (Marcel *et al.*, 2014). When travelling across borders, some criminals use fake identity documents to avoid detection and apprehension.

Online, criminals use pseudonyms and online personas to commit offenses and avoid apprehension. A pseudonym, or the identity of an online persona, is an example of virtual identities, i.e. the

identity of a virtual entity linked to the actual entity of interest. For instance, a sex offender posed as a young girl to befriend victims and introduce them to the offender himself in order to create false trust. As another example, criminals gain unauthorized access to bank accounts by stealing account details that are used to identify the owner. The various ways in which identity can be changed (usurped, exchanged, delegated, created) creates complexities for security, investigations, and law (Koops *et al.*, 2009).

There are legitimate reasons to change or 'spoof' identity. People also use pseudonyms to protect their official identities. For instance, famous people use pseudonyms to protect their privacy. People use virtual identities or personas in cyberspace in order to operate anonymously. From yet another perspective, forensic analysts might attempt to spoof the fingerprint authentication on a smartphone in order to acquire data from the device, or use a virtual identity for a covert investigation.

Forensic methods sometimes enlarge the gap between identifying information and the actual thing, such as when imperfect preservation techniques are applied in dynamic crime scene environments, or when experimental studies are performed under controlled conditions. Digital traces are further separated from the physical entity generating them, so establishing a link between them requires assumptions which necessarily have some additional uncertainty. Furthermore, errors in processing and comparison can result in mistaken identity, even with DNA, such as contamination that leads to incorrect conclusions (Geddes, 2012).

With such uncertainties in mind, recall the different aspects of identity listed in Table 2: something you are (biometric features), something you have (token, certificate), something you know (PIN, password), and something you do/prefer. A confluence of corroborating physical and digital traces from multiple independent sources can help establish what will be interpreted as an undeniable identity, as in the Graham Dwyer case summarized above. Given the multifaceted nature of identity, it can be difficult to evaluate the level of confidence in a formal manner. Ultimately, the reliability of any identification process depends on the competence, honesty, and belief of forensic analysts (Jaquet-Chiffelle, 2009). Proper assessment of identification assumes that the forensic analyst performing the work has the necessary knowledge and abilities, has taken potential biases into account and, ultimately, is trustworthy.

Evaluating and expressing confidence in identity

A common goal of investigating criminal activity is to apprehend the perpetrators, and make them accountable for their crimes. At the same time, to avoid injustice, it is necessary to seriously consider the possibility that the accused is innocent. Forensic analysts have a duty to resist pressures to target a specific entity when evaluating identity, and avoid confirmatory bias. Specifically, when evaluating and expressing forensic results, forensic analysis should focus on the observable physical and digital traces, and not be aimed at implicating a specific entity (Association of Forensic Science Providers, 2009).

Evaluating possible associations between identity characteristics and a specific entity is not as straightforward as it might seem. Many characteristics provide some partial information about an entity, but it is difficult to quantify how reliably a given characteristic can be linked to a single entity. The possibility exists that two people have very similar hair or fingerprints, so a forensic analyst could mistakenly identify the wrong person. Certain information is perceived as more reliable for establishing identity because it is more difficult to alter (e.g. something you are). However, the stability of such identity-related information can make it more of a target for identity usurpation (Koops *et al.*, 2009). Therefore, the authenticity of such information must be assesses when it is used to establish identity, rather than simply assuming that it is reliable.

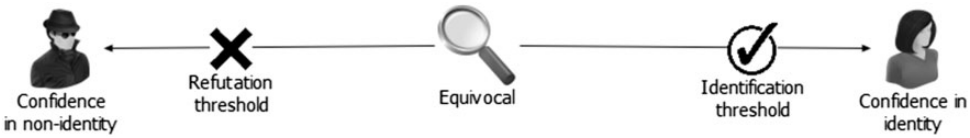

Figure 2: Decision about identity with thresholds for establishing identity (sufficient confidence in identity) versus refuting identity (sufficient confidence in non-identity) adapted from Jaquet-Chiffelle (2009).

It is sometimes possible to establish sufficient confidence that 'some given identity-related information is valid and truly describes only one specific entity in the given context, [and] then this entity is (fully) identified, i.e. *individualized*, with this information in this context from the point of view of the [decision-maker]. If the [decision maker] convinces himself that other entities can be truly described by this information in this context, then the identification is only partial from his point of view.' (Jaquet-Chiffelle, 2009)

The determination of what confidence level is sufficient for establishing identity in a given context involves setting thresholds. Fig. 2 depicts these thresholds of confidence in identity on a continuum with confidence in non-identity (refutation or distrust) to the left, confidence in identity to the right, and equivocal or neutral (lack of confidence) in the middle. The level of confidence can also be represented using an 'opinion triangle' to support more formal expression and opinion algebra (Jaquet-Chiffelle, 2009).

Over the past 100 years, there have been significant advances in the study of traces that can be used to address questions of identity. However, many of these advances in forensic science have not adequately addressed questions of reliability. In recent years, there is increasing concern regarding unreliability of certain forensic observations for purposes of establishing identity, and growing awareness that methods of establishing identity do not provide absolute certainty (National Research Council, 2009). For instance, mistakes in bite-mark analysis have led to dozens of wrongful convictions, calling into question the reliability of methods for comparing bite-marks to a suspect's teeth (Lussenhop, 2016). Similarly, an FBI study found that over 250 cases (95% of the total number of cases that were reviewed) involving hair evidence had errors in expert testimony, raising questions about the reliability of hair evidence for identifying a person (Hsu, 2015; Norton *et al.*, 2016). Concerns about the reliability of fingerprint evidence have also arisen in cases of mistaken identity, in large part due to errors in the comparison process (Cole, 2005; Stockdale *et al.*, 2012) . As more misuses of forensic science are uncovered, higher scrutiny and expectations are being placed on forensic science as a whole (Garrett and Neufeld 2009).

In addition to on-going efforts to improve forensic methods to support identification, there are multiple initiatives to standardize how conclusions are conveyed. The primary motivation for these efforts is to eliminate ambiguous language such as the assertion that an observation of a trace at the crime scene 'is consistent with' a particular person being at the crime scene. When a person's liberty and livelihood are at stake, or a dangerous criminal could remain free and cause further harm, it is critical to use unambiguous language to state the level of compatibility between a trace and its purported source, weighed against alternative propositions.

Some groups use conclusions scales that have a defined vocabulary to express confidence in forensic results. One risk of using a conclusion scale is that it can be used to target one entity, such as stating that there is strong support for a given entity given the observed traces, effectively favouring one conclusion by not formally including an evaluation of any alternate hypothesis. To address this risk, the Organization of Scientific Area Committees is developing guidelines for source

conclusions that uses comparative language to express the support for one proposition compared with the support for the opposite proposition.

To increase scientific rigour in forensic science, there is an on-going effort to express conclusions about identification as an expert decision in terms of comparison of likelihoods (ENFSI, 2015). The first evaluation is the strength or weight of the forensic observations given one account of the alleged fact (generally the prosecution's account) and the second asks for the weight of the forensic observations given an alternative account of the events (generally the defense alleged set of facts). For instance, the likelihood ratio in favour of an identity increases when there is a strong chance of making the observations given the alleged identity and a small chance of making these observations if an unknown individual is at the source of the data. This approach gives decision makers a basis for assessing confidence of identification results that is more formalized and numerical instead of a verbal conclusion scale (Marquis et al. 2016).

The *Ecole des Sciences Criminelles* (ESC), School of Criminal Justice, takes the stance of not giving an implicit message of a factual certainty when reporting conclusions related to identity, or that the results alone can achieve 100% certainty or definitively exclude any other alternative scenario. Research and casework at the ESC are striving to develop more effective ways to evaluate and express the probative value of forensic findings. This focus spans across physical and digital realms, from fingerprints and handwriting to mobile devices and the Internet of things (IoT).

Relationships between material and digital/virtual identities

When it comes to attributing specific activities to a human being, digital data has advantages and disadvantages over physical traces such as DNA and fingerprints.

Although DNA and fingerprints have the advantage of being physical in nature, they usually lack contextual details such as when and how they came to be in a particular place. For instance, finding a fingerprint may be used to establish that a person was present at a particular place, but not when. Conversely, digitized fingerprints can have contextual details, including when they were generated and used, providing more information to establish identity. For example, a biometric authentication system not only records the presence of a fingerprint, but also the time. Actually, some smartphones contain a combination of biometric, location, and temporal details that can be useful for establishing the identity of the user. Some financial services check the geolocation of where a transaction originates, and generate an alert when a transaction occurs far away from the customer's usual or expected location.

Furthermore, certain biometric features only exist when they are recorded, such as the human voice. When investigating criminal activities involving virtual entities, being able to capture their voice can provide a strong link to the human being committing the offenses.

> Case example: In criminal investigations, it may be possible to link a human being to biometric information found in digital traces, such as a voiceprint or fingerprint. In one child sexual assault case, the offender was linked to the offense by analysing a fingerprint that was captured in one digital photograph he had taken of a victim. (Augenstein, 2015)

Prior to widespread use of anonymizing technology such as The Onion Router (Tor), online activities could be tracked back to the Internet Service Provider account (virtual entity) on the basis of the IP address used during the time period. Internet Service Providers (ISP) could provide law enforcement with the customer details for the Internet account, and sometimes the phone

number used to connect at the specific time. This type of information has been used extensively in criminal investigations to establish the identity of the human being who performed the crime.

> Case Example (Travis, St. Louis, 2002): Maury Roy Travis, who was convicted for serial homicide, was apprehended after he sent a letter to a reporter that contained a map generated from a website (Bryan, 2002). The act of plotting a map left a cybertrail that law enforcement used to determine the ISP account used to generate the online map, and with the help of ISP records, the name and address of Travis. Some surveillance of Travis's home was performed to establish confidence that he was the actual person being sought.

Even with the advent of virtual currencies such as BitCoin that support pseudonymity, these systems retain detailed records of all transactions. When BitCoins are used for illegal purposes, investigators can sometimes identify the perpetrator by determining the owner of the associated wallet. In other cases, investigators have identified the thief when he transferred the BitCoins into currencies in the physical world (Jeong, 2015).

Mobile devices and smartphone apps generate substantial amounts of geolocation information, on the device itself, and on cellular and cloud service provider networks. Such information associated with a specific subscriber's mobile device can be used to track an individual's movements over time.

There are subtle errors that can arise while following cybertrails, such as mistyping the IP address when requesting ISP records, or specifying the wrong timezone. Geolocation information on mobile devices can be inaccurate due to variations in signal quality or sampling, and can be intentionally altered using a GPS spoofing app. Errors in digital traces can result in law enforcement mistakenly searching the wrong location and interrogating the wrong person. Geolocation data from cell towers (or mobile devices, vehicles, etc.) might indicate that a given suspect was near the crime scene at a given time. However, bias and mistakes can occur when analysis only considers 'a prosecution hypothesis when there is a defence hypothesis available, or [optimise the] likelihood of detecting all serving cells when surveying a location highlighted by the instructing agency while providing a cursory examination of alternative scenarios, for example an alibi location.' (UK Forensic Science Regulator, 2015). Complexities also arise when multiple people share a virtual identity such as a mobile device, vehicle, computer, IP addresses, or Internet account.

Linking a virtual person to a physical one can become much more challenging. It is necessary to address the questions: How do we know we have the right person? How do we know that the identified person is the actual source of the activity? Stated in terms of a likelihood ratio, what is the likelihood that we have the right person, versus the likelihood that we have the wrong person? Furthermore, with the increasing amount of identity usurpation, it is also necessary to consider the question: How do we know if someone has 'stolen' an identity?

In some circumstances, it can be difficult to establish a link between digital activities and a physical entity with sufficient confidence for forensic purposes, particularly when dealing with criminals who are actively trying to avoid apprehension. However, computer systems have the advantage of being copious. Ubiquitous devices retain substantial amounts of detailed information about physical and virtual activities that can provide high and low selectivity characteristics useful for establishing identity.

A powerful approach to establishing relationships between material and digital/virtual identities is to combine digital traces with traditional police work, as well as traditional forensic analysis methods. When investigating sale of illegal substances

via the Internet, forensic analysis of the materials correlated with both physical and online selling sources can provide a more complete reconstruction of the criminal organization (Pineau *et al.*, 2015). When bank thieves equip cash machines with skimming devices, the only way to identify the offenders might be to perform physical surveillance until they come back to collect stolen information. As demonstrated in the Graham Dwyer case, combining multiple forensic disciplines can be very effective when trying to establish identity in violent crime investigations. The ESC emphasizes this transdiciplinary approach, integrating forensic science disciplines in teaching, research, and expertise in the forensic laboratory supporting casework in criminal matters. This coordinated approach recognizes that a case cannot usually be solved by one piece of information alone, and that the concept of identity in our modern society must take into account both physical and digital traces.

Growing concerns: privacy and illegal access to identity information

The exposure of identities to criminals, governments, and private industry is an increasing concern. Given the number and size of data breaches and rising risk of government surveillance, it is reasonable to assume that everyone has had some identity-related information stolen or monitored. In response to these risks, commercial ventures such as Evernym.com are developing systems to provide enhanced security and control over virtual identities. Governments are also addressing these concerns with updated legislation. In 2014, the European Court of Justice (ECJ) held that the 2006 EU Data Retention Directive breaches the 'citizens fundamental rights to respect for private life and communications and to the protection of their personal data' (EU Court of Justice, 2014). In an effort to overturn his conviction for murder, Graham Dwyer is using this ECJ decision to challenge the legality of the use of digital traces that helped establish his identity. In 2016, the EU General Data Protection Regulation (GDPR) was approved in an effort to address deficiencies in prior legislation.

There are also growing concerns that identities might be linked to the incorrect person, particularly with virtual identities. As illegal access to identity information becomes more prevalent in the digital age (passport numbers, ID cards, bank accounts), there is rising risk that activities will be performed by an impersonator using stolen identity information or biometric spoofing. Questions of reliability in virtual identity and partial identity using digital traces will continue to be a challenge in the decades ahead.

Furthermore, the majority of people do not take precautions to protect their online activities. As a result, there are increasing opportunities for analysts to link people with something they do or like. Businesses are sharing customer information for marketing purposes, aggregating previously separated aspects of our lives, such as banking activities combined with shopping patterns. As a result, commercial organizations can analyse digital activities and identities to learn more about consumer habits and to target online marketing. This kind of data analysis and categorization is not necessarily accurate and can impinge upon personal privacy (Ellenberg, 2014). Similar data analysis methods can be useful in criminal investigations, but there are growing concerns over bulk data collection and government surveillance. Proponents of the UK Investigatory Powers Act 2016 claim that broad access to digital data by governmental entities is necessary for security, whereas opponents claim that this unprecedented access is not proportionate and encroaches too much on privacy.

Recommendations for updated legislation and policy have emerged the FIDIS (The Future of Identity in the Information Society) EU Project in an effort to address these complex challenges,

including identity-related crime (Koops *et al.*, 2009).

Conclusions

Identities do matter, both from a policing perspective and for the future of society in a digital age. Identity is earning significant attention in forensic science, with questions about reliability of existing methods to establish identity, and emerging challenges posed by new technology. Forensic scientists are working to increase the reliability of current identification techniques, and to develop new methods for establishing identity using digital traces, and clearer ways to express conclusions about the confidence of an identity. At the same time, heightened awareness of data breaches and government surveillance is motivating governments and companies to address concerns about privacy and illegal access to identity information. If these efforts are successful, forensic scientists, governments, and commercial organizations will have more powerful ways to establish identity combining physical and digital information. As more identity information is collected into databases, consideration must be given to the increased probability of coincidental collisions, and ways to mitigate such risk such as maintaining separate smaller databases for specific purposes. In addition, controls must be placed around identity information to protect privacy and security. The future will bring new challenges—storing and sharing more identity information will continue to have risks of misuse and misidentification. The pluridisciplinary approach of the ESC combines forensic disciplines to obtain a stronger comprehension of identity. The resulting insights are critical in forensic science and can support broader applications in society, particularly with the increasing reliance on virtual identities for protecting safety and privacy. Always keep in mind that identification is a decision process with a threshold, not an absolute certainty.

Acknowledgements

We would like to thank Christophe Champod for sharing his strong experience with forensic analysis physical traces and being an invaluable guide in the study of the differences and relationships between physical and virtual identity. Our deep appreciation also goes to Jean-Luc Gremaud for his thoughtful work, comments, and encouragement.

References

Association of Forensic Science Providers (2009). 'Standards for the Formulation of Evaluative Forensic Science Expert Opinion.' *Science and Justice* **49**(3): 161–164 (http://dx.doi.org/10.1016/j.scijus.2009.07.004).

Augenstein, S. (2015). 'Fingerprint ID from a Photograph Leads to Child Porn Conviction, Digital Reporter.' *ForensicMag*, 26 June 2015. http://www.forensicmag.com/article/2015/06/fingerprint-id-photograph-leads-child-porn-conviction/ (accessed 9 May 2017).

Biedermann, A., Bozza, S. and Taroni, F. (2016). 'The Decisionalization of Individualization.' *Forensic Science International* **266**: 29–38.

Bryan, B. (2002). 'Letter Writer is Serial Killer, Concludes Criminal Profiler.' St. Louis Post Dispatch, 28 May 2002.

Champod, C. and Evett, I. W. (2001). 'A Probabilistic Approach to Fingerprint Evidence.' *Journal Forensic Identification* **51**: 101–122.

Champod, C. (2013). 'Overview and Meaning of Identification/Individualization.' In Siegel, J. A., Saukko, P. J. and Houck, M. M. (eds.), *Encyclopedia of Forensic Sciences*, Second Edition, Waltham: Academic Press, pp. 303–309.

Cole, S. A. (2005). 'More than Zero: Accounting for Error in Latent Fingerprint Identification.' *The Journal of Criminal Law and Criminology* **95**(3): 985–1078.

Cole, S. A. (2009). 'Forensics Without Uniqueness, Conclusions without Individualization: the New Epistemology of Forensic Identification.' *Law, Probability and Risk* **8**: 233–255 (doi:10.1093/lpr/mgp016)

Coquoz, R. and Taroni, F. (2006). *Preuve par l'AND: La Génétique au Service de la Justice*, 2nd edn. Lausanne: Presses polytechniques et universitaires romandes, p. 136–139.

Ellenberg, J. (2014). 'What's Even Creepier Than Target Guessing That You're Pregnant?' *Slate*, 9 June 2014 http://www.slate.com/blogs/how_not_to_be_wrong/2014/06/09/big_data_what_s_even_creepier_than_target_guessing_that_you_re_pregnant.html/ (accessed 9 May 2017).

ENFSI (2015). '*ENFSI Guideline for Evaluative Reporting in Forensic Science*.' European Network of Forensic Science Institutes, Dublin. http://enfsi.eu/wp-content/uploads/2016/09/m1_guideline.pdf/ (accessed 9 May 2017).

EU Court of Justice (2014). 'The Court of Justice declares the Data Retention Directive to be invalid.' Judgment in Joined Cases C-293/12 and C-594/12: Digital Rights Ireland and Seitlinger and Others. http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf/ (accessed 9 May 2017).

Garg, R., Hajj-Ahmad, A. and Wu, M. (2013) 'Geo-location Estimation from Electrical Network Frequency Signals.' In ICASSP, Vancouver, BC, Canada, pp. 2862–2866.

Garrett, B. L. and Neufeld, P. J. (2009). 'Invalid Forensic Science Testimony and Wrongful Convictions.' *Virginia Law Review* **95**(1): 1–97.

Geddes, L. (2012). 'How DNA Contamination can Affect Court Cases.' *New Scientist*, 11 January 2012. https://www.newscientist.com/article/mg21328475-000-how-dna-contamination-can-affect-court-cases/ (accessed 9 May 2017).

Gremaud, J. L. (2010). *Processus de reconnaissance et d'identification de personnes décédées. Thèse de doctorat, Ecole des Sciences Criminelles*, University of Lausanne.

Hsu, S. S. (2015). 'FBI Admits Flaws in Hair Analysis Over Decades.' *The Washington Post*, 18 April 2015. https://www.washingtonpost.com/local/crime/fbi-overstated-forensic-hair-matches-in-nearly-all-criminal-trials-for-decades/2015/04/18/39c8d8c6-e515-11e4-b510-962fcfabc310_story.html/ (accessed 9 May 2017).

Inman, K. and Rudin, N. (2002). 'The Origin of Evidence.' *Forensic Science International* **126**: 11–16.

Jackson, G., Jones, S., Booth, G., Champod, C. and Evett, I. W. (2006). 'The Nature of Forensic Science Opinion—a Possible Framework to Guide Thinking and Practice in Investigation and in Court Proceedings.' *Science & Justice* **46**(1): 33–44.

Jaquet-Chiffelle, D.- O. (2009). 'Identification.' In Jaquet-Chiffelle, D.-O. and Buitelaar, H. (eds), *Section 4.2 in Trust and Identification in the Light of Virtual Persons, FIDIS deliverable 17.4.* (http://www.fidis.net/fileadmin/fidis/deliverables/new_deliverables/fidis-wp17-del17.4_Trust_and_Identification_in_the_Light_of_Virtual_Persons.pdf).

Jeong, S. (2015). 'Criminal Charges Against Agents Reveal Staggering Corruption in the Silk Road Investigation.' *Forbes*, 31 March 2015. http://www.forbes.com/sites/sarahjeong/2015/03/31/force-and-bridge/ (accessed 9 May 2017).

Kirk, P. L. (1963). 'The Ontogeny of Criminalistics.' *Journal of Criminal Law and Criminology* **54**(2): Article 17.

Koops, B.- J., Leenes R., Meints, M., van der Meulen, N. and Jaquet-Chiffelle, D. -O. (2009). 'A Typology of Identity-related Crime: Conceptual, Technical, and Legal Issues.' *Information, Communication & Society* **12**(1): 1–24.

Lussenhop, J. (2016). 'Can you Catch a Killer Using Only Teeth Marks?' *BBC News*, 15 February 2016. http://www.bbc.com/news/magazine-35564041/ (accessed 9 May 2017).

Marcel, S., Nixon, M. S. and Li, S. Z. (2014). *Handbook of Biometric Anti-Spoofing*, London: Springer.

Marquis, R., Biedermann, A., Cadola, L., Champod, C., Gueissaz, L., Massonnet, G., Mazzella, W. D., Taroni, F. and Hicks, T. (2016). 'Discussion on how to Implement a Verbal Scale in a Forensic Laboratory: Benefits, Pitfalls and Suggestions to Avoid Misunderstandings.' *Science & Justice* **56**(5): 364–370.

McMenamin, J. (2006). 'Video Account of Killing Shown.' *Baltimore Sun*, 30 November 2006. http://articles.baltimoresun.com/2006-11-30/news/0611300202_1_gaumer-cell-umbc/ (accessed 9 May 2017).

McMenamin, J. (2007). 'Gaumer Convicted of Rape, Murder: Prosecutors Seeking Death Penalty for UMBC Student, who met Victim Online.' *Baltimore Sun*, 10 May 2007. http://articles.baltimoresun.com/2007-05-11/news/0705110217_1_gaumer-umbc-phone-records/ (accessed 9 May 2017).

Norton, J., Anderson, W. E. and Divine, G. (2016). 'Flawed Forensics: Statistical Failings of Microscopic Hair Analysis.' *Significance* **13**(2): 26–29. (doi:10.1111/j.1740-9713.2016.00897.x).

National Research Council (2009). *Strengthening Forensic Science in the United States: A Path Forward*. Washington, D.C.: The National Academies Press.

Pineau, T., Schopfer, A., Grossrieder, L., Esseiva, P. and Rossy, Q. (2015). 'Internet Forums: A Source of Intelligence to Monitor the Online Diffusion of Doping Products' presented at DFRWS EU 2016. http://www.dfrws.org/conferences/dfrws-eu-2016/sessions/internet-forums-source-intelligence-monitor-online-diffusion/ (accessed 9 May 2017).

Raidió Teilifís Éireann (2015). 'How Gardaí Built the Case against Graham Dwyer.' *RTE News*, 27 March 2015. http://www.rte.ie/news/2015/0327/690272-garda-case-against-graham-dwyer/ (accessed 9 May 2017).

Robertson, B., Vignaux, G. A. and Berger, C. E. H. (2016) *Interpreting Evidence: Evaluating Forensic Science in the Courtroom*, 2nd edn, Chichester: Wiley.

Stack, S. (2015). 'Graham Dwyer Trial: The 14 Points that led to Graham Dwyer's Arrest.' *The Irish Independent*, 27 March 2015. http://www.independent.ie/irish-news/courts/graham-dwyer-trial/graham-dwyer-trial-the-14-points-that-led-to-graham-dwyers-arrest-31091054.html/ (accessed 9 May 2017).

Stockdale, M., Carr, S. and Wortley, N. (2012). 'The Scottish Fingerprint Inquiry's Ramifications for England and Wales (Part 1).' *Criminal Law and Justice Weekly*, 27 January 2012. https://www.criminallawandjustice.co.uk/features/Scottish-Fingerprint-

Inquiry%E2%80%99s-Ramifications-England-and-Wales-Part-1/ (accessed 9 May 2017).

SWGFAST (2013). 'Guideline for the Articulation of the Decision-Making Process for the Individualization in Friction Ridge Examination (Latent/Tenprint).' Document #4. http://clpex.com/swgfast/documents/articulation/130427_Articulation_1.0.pdf/ (accessed 9 May 2017).

Teh, P. S., Teoh, A. B. J. and Yue, S. (2013). 'A Survey of Keystroke Dynamics Biometrics.' *The Scientific World Journal* 2013. (doi: 10.1155/2013/408).

UK Forensic Science Regulator (2015). 'Codes of Practice and Conduct, Appendix: Digital Forensics – Cell site analysis.' Consultation Outcome FSR-C-214. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/486289/2015_12_15_FSR-C-214_Cell_site_consultation_draft.pdf/ (accessed 9 May 2017).

UK Investigatory Powers Act 2016. (http://www.legislation.gov.uk/ukpga/2016/25/contents/enacted/data.htm/ (accessed 9 May 2017).

Wasser, S. K., Brown, L., Mailand, C., Mondol, S., Clark, W., Laurie, C. and Weir, B. S. (2015) 'Genetic Assignment of Large Seizures of Elephant Ivory Reveals Africa's Major Poaching Hotspots.' *Science* **349**(6243): 84–87 (doi: 10.1126/science.aaa2457).