Digital transformations in forensic science and their impact on policing

Olivier Ribaux[*], Olivier Delémont, Simon Baechler, Claude Roux, Frank Crispino

[*]Corresponding author:
Olivier Ribaux
University of Lausanne
Batochime
CH 1015 Lausanne Dorigny
olivier.ribaux@unil.ch

Abstract

The technologies used in forensic science are now more easily transportable, fast and useable in the field by non-specialists. They help detect, collect and analyze a large volume of new and more diverse traces generated by criminal activities. These changes, in order of magnitude, induce the rapid digital transformations of forensic processes, requiring, in turn, a radical shift in roles and tasks within traditional forensic and police structures, as well as in the criminal justice system as a whole. In this chapter, examples are presented to help characterize these developments that are subject to many tensions. The new situation and its complexity prompt interrogations about the suitability of a law enforcement paradigm of policing that mainly define the scope of forensic science as an ancillary to the Criminal Justice System. The current context offers instead many opportunities to express the value of forensic thinking in proactive policing. Traceology, as the science of traces, is proposed as the overarching approach to pave the way for balanced, regulated and efficient approaches to intelligence and policing.

Keywords: forensic intelligence; traceology; crime analysis; digital transitions.

Introduction

The shift from a reactive approach to crime, to a pre-crime conception based on risk analysis, is a major direction in policing observed in criminology (Zedner, 2007). It relies on the analysis of accessible information to prevent new occurrences or mitigate the unpleasant effects of recurrent behaviors outside certain norms (*e.g.* problem-oriented, intelligence-led). It provides a new management style, led to structural reforms, changed recruitment and intensified networking between public and private actors.

As budget reduction can better restrain police role to traditional enforcement models, which is considered as 'the real police work' (Keay & Kirby, 2018), services adopting this proactive policing approach should prioritize the most efficient action plans for preventing and disrupting crimes, or reducing harm it may cause. To this end, there is an evolution to make them more evidence-based (Ratcliffe, 2016; Weisburd & Majmundar, 2018).

Whatever the restrictive or proactive policing path followed, security systems are subjected to many tensions.

Forensic science has primarily positioned itself as a service provider to the criminal justice system, or is at least considered that way by many authors and even practitioners. Hence, the forensic science community seems relatively indifferent to evolutions in policing (Roux, Talbot-Wright, Robertson, Crispino, & Ribaux, 2015). Police managers, in general, do not perceive the potential and sufficient reasons for promoting an expanded use of forensic science in proactive policing models (see also chapter 9 - Crispino et al).

As crime and security problems evolve in nature and scale (e.g. concentrations of crime and its seriality are better assessed), technologies are being used in a widespread and decentralized manner, enabling new levels of surveillance, the networking of police and forensic databases, and the intelligent processing of large data sets generated by widespread human traceability (Casey, 2019; Casey, Ribaux, & Roux, 2019). This trend is captured as digital transformations and requires a change of mentality.

While emphasizing how forensic science remains locked into the reactive policing model imposed by the criminal justice system, we will first analyze the progressive extension of the use of DNA profiles using networked databases as an example of how digital transformations are changing the scale at which many forensic processes are applied.

The ability of the standard law enforcement model, with its narrow view of forensic science, to absorb such expanding flows and together provide an added-value in policing will be questioned.

We will then observe that digital forensics has progressively emerged within police organizations (Pollitt, 2010). Digital traces became so ubiquitous and new problems so varied that the digital forensics community has found itself at the center of these tensions and pivotal to the reflection on policing models. Digital forensics, conceived firstly as a narrow technical support to forensic processes, has expanded to implement early applications of digital traces in investigations. These applications now include the rapid treatment of new volumes and varieties of traces in specific cases, and the development of new forms of intelligence and crime analysis processes for dealing with cyberfrauds or other forms of crimes exploiting digital infrastructures.

This unanticipated expansion of their role supports the view that forensic science, integrating physical and digital traces, is a solid foundation for reframing a science of policing, implementing new kinds of digital policing that balances the consideration of various relevant dimensions and perspectives. This requires cross-cutting and evidence-based attitudes (Weisburd & Neyroud, 2013), incorporating the basic principles and lessons learned from forensic science (Casey, 2019). Such an evolution is in opposition to the proliferation of specializations, and the risks of fragmenting and complexifying the practice of policing in the digital age.

Forensic science as a service to the criminal justice system

Forensic science is currently under fire from critics. Its negative role in spectacular cases of miscarriages of justice has been repeatedly established. The FBI's false identification of Brandon Mayfield using a fingermark collected after the Madrid terrorist attack in 2004 served as a catalyst. This incredible mistake has largely initiated a strong movement over the past decade to challenge forensic science as a whole (NAS, 2009; PCAST, 2016).

One of the unintended effects of this movement is that it inhibits the development of a broader vision for forensic science. In a simplified way, the derived research in forensic science since largely focuses on how to strengthen forensic processes, mainly by re-enforcing quality controls. The evaluation of forensic information for supporting decisions of a Court of law attracts all the interest, because it is where miscarriages of justice are most dramatic. This movement insatiably leads forensic organizations to further specializations defined around the use of sophisticated and rapidly changing technologies. The focus is on the means (technologies and separated processes), rather than on problems to be solved.

There are two changes here brought by digital transformations. Firstly, digital traces exacerbate the confusion about the positioning of forensic science as an integrated branch of the police or as an auxiliary to the justice system (Baechler et al., 2020). Traces extracted from electronic devices are used extensively early in investigations. In parallel with the movement of decentralization and commoditization of other types of more conventional analysis (*e.g.* rapid-DNA, live scan, breath-analyzer), the investigative aspect is reinforced on a new scale (Casey et al., 2019). This situation makes the position of the traditional forensic laboratories more problematic, because they are supposed to operate independently and on request, mostly on an evaluative basis for the justice system. This is occasionally imposed by a specific law. Within their usual framework, they find it difficult to integrate the timely, collective and tacit nature of the investigation's reasoning.

Despite this changing context, policing models are still not really on the agenda of the normative forensic science community. This is in contradiction with real forensic practices undertaken at the level of the police, which are influenced by crime analysis models (*e.g.* understanding involved entities, modus operandi, hence, able to link crimes, bring knowledge on criminal networks) (Bradbury & Feist, 2005; Tilley & Ford, 1996).

An account of the evolution of DNA technologies will allow for further analysis of how forensic processes are designed from a law enforcement perspective, despite evidence that digitization requires integration with other policing strategies.

Digital transformations: the example of the successive evolutions of DNA technologies

A specific area of development in forensic science has been the increasing use of so-called identification databases. Automated Fingerprint Identification Systems (AFIS), and then DNA databases (generally known as CODIS) serve as milestones in the digitalization process. Their intensive use is expected to increase the volume of identifications of persons with a view of combating cross-border crimes and terrorism (Toom, 2018)[1]. The implicit assumption is that increased identification possibilities would have a direct and obvious effect on the mitigation of all kinds of crime. However, it is far from being so simplistic in policing (Ratcliffe, 2016).

[1] See also the European Network of Forensic Science Institute's (ENFSI) strategy for 2017-2020 http://enfsi.eu/wp-content/uploads/2017/11/4.0-ENFSI-Strategic-Plan-2017-2020.pdf (accessed 3rd January 2019)

Beyond the important stage of database implementation, many other significant advances in the field of DNA technology have raised fundamental, often unexpected questions about the functioning of the criminal justice system and its relationship with forensic science.

We will divide the analysis of these developments into two parts. The first concerns the evolution of DNA processes from the early ages of technology to the present day. In the second part, we will examine how database networking is currently changing orders of magnitude in the number and nature of matches obtained and what these changes mean in terms of policing. This analysis will raise the general question of the adequacy of the law enforcement policing model to interpret forensic activities.

a. Successive transformations from the inception of the technology

The use of DNA in forensic science originates from the mid-80s. The exploitation of new type of information extracted from biological traces expanded in an unprecedent way possibilities of investigating both serious crimes and high-volume crimes. This new technology was first used punctually to exclude or point to a possible suspect and to indicate the activity of serial perpetrators in high profile cases. It is since the mid-1990s that DNA profiles have been more widely exploited through the establishment of systematic, database-supported processes. These developments just followed the advent of Automated Fingerprint Identification Systems (AFIS). The two digitalized forensic identification processes (CODIS for DNA and AFIS) have enhanced the contribution of forensic science to investigations. However, at the same time, they have changed the volume of data flows in orders of magnitude, resulting in unanticipated problems and more fundamental changes in the criminal justice system as a whole.

Indeed, enthusiasm was rapidly tempered by the unanticipated consequences of the growth of databases. In the design of the first DNA databases in the 1990s, adventitious matches became statistically inevitable as the number of profiles submitted increased. The consequences were highlighted when Raymond Easton ran into difficulties in the United Kingdom in 1999. A profile extracted from one specimen collected from a burglary matched adventitiously his DNA profile stored in the database. Confidence in the DNA-process was so high, wrongly, that he was prosecuted for burglary. The responses were to improve the quantity and quality of the data stored on each DNA profile, as well as to strengthen the interpretation of matches using statistical and probabilistic approaches. In parallel, a new technological breakthrough has increased the sensitivity of DNA extraction techniques. This increased the proportion of DNA profiles extracted from difficult traces collected from the scene of crime (Castella & Mangin, 2008). These hard-to-interpret profiles (partial or mixture) now make up most of the data in some databases that have, moreover again grown. The difficulty of the interpretation process has added new levels of complexity in the use of DNA flows. However, these progresses came with greater specialization and added a level of complexity to the entire criminal justice system. DNA specialists were in charge of collecting and extracting DNA profiles, as well as interpreting results. They developed their own methodologies and distributed roles and tasks in various forms of independent organizations across countries. In particular, specialization has created greater divisions in the entire investigative process hindering communication of information and knowledge transfer. New failures due to this complexity started to emerge, for example, in the Jama case in Australia (Vincent, 2010). Farah Jama was wrongly convicted of rape on the basis of a (true) DNA match detected and misinterpreted in an incredible set of circumstances generated by fragmented DNA and investigative processes.

Other developments have allowed the expanded use of DNA and added a level of complexity, such as the so called familial searches, *i.e.* the way criminals are identified via relatives found by similarities in DNA profiles (Bieber, Brenner, & Lazer, 2006). This novelty brought many success stories, mainly in conjunction with the use of national DNA databases (Maguire, McCallum, Storey, & Whitaker, 2014; Pham‐Hoai, Crispino, & Hampikian, 2014). More recently, publicly available genetic data have been used along the same lines, but with more complex data involving distant familial relatives. This investigative initiative led, inter alia, to the identification of the 'Golden State Killer', Joseph James DeAngelo, having perpetrated a series of murders and assaults dating back more than 30 years, in California (Scudder, Robertson, Kelty, Walsh, & McNevin, 2018). Besides, the risks to human rights and privacy have become progressively more concrete with the scale of these forensic transformations and the impact of such spectacular illustrations (Erlich, Shor, Pe'er, & Carmi, 2018; Mc Cartney, 2006). This has also led to different legal frameworks and decision-making processes in the area of law enforcement, which explains why DNA-related processes take place very differently from one country to another.

At the same time, DNA processes quickly faced backlogs. For certain databases, results were delivered only in four to six months. This made the database inoperative in relation to the pace of investigations, and much DNA data was unexploited (Strom & Hickman, 2010). This led to two reactions. Firstly, the size of the infrastructures has been increased to absorb a larger flow, requiring new resources. Second, in parallel with budget concerns, a stronger triage process was also defined prior to submission to a DNA laboratory for the extraction of a profile. This has also led to new questions, such as defining the characteristics of a relevant trace to submit (Bitzer, Delémont, & Ribaux, 2016). Criteria chosen emphasized the typical influence of the law enforcement model. The severity of the cases involved as well as the quality of the specimen collected (for example, the quantity of biological material collected) are the main incentive to submit a trace. Pertinence and seriality are generally a much less important concern (Bitzer et al., 2016).

Another innovation disrupted the process: rapid DNA technologies can extract, in less than two hours, a profile taken from a person or from a specimen in a standalone manner. This makes it possible to decentralize the process, making it more systematic and timelier. It is a likely trend that challenges the infrastructures developed in the central laboratories to absorb the growing flows.

The second concern was to absorb a flow of data into an economically acceptable model. Choices are then obviously linked to what can be considered as the overall "efficiency" of these processes. This is generally measured in terms of proportions of cases investigated where a trace has led to identification. This is typically derived from a law enforcement model focused on resolution rates. In such evaluations, an attrition gives an embarrassing picture making it difficult to justify costs by a level of efficiency: from many traces collected at the scene, very few play a role in the ultimate decision making in Court. Contrary to what was intuitively expected, end-to-end studies show that very few scenes attended concerning high volume crimes lead to the identification of a suspect (1-2 % for DNA traces and fingermarks) (Brown & Ross, 2012).

These kinds of analysis thus lead to further questions about the use and integration of DNA databases as a component of the whole criminal justice and security system. It was occasionally recognized that:

“A lack of integration between the DNA laboratories and the other components of the justice system responsible for following up on results is perhaps the biggest weakness, in that desirable outcomes have not been clearly defined or carefully researched” (Bieber, 2006, p. 231).

Surprisingly, instead of focusing on such fundamental issues, there seems to be a compelling trend towards full computerization of DNA processes as part of the broader vision called Streamlined Forensic Reporting (SFR). This managerial vision, which does not require to challenge the law enforcement policing model, goes directly from the trace to its use by the justice, renouncing all intermediate investigations usually resulting from matches (Mc Cartney, 2019)[2].

b. Networking of databases as a further expansion

Another wave of complexification is coming: DNA databases infrastructures are being networked at an international level. In particular, in Europe, the 2005 Prüm treaty was signed between seven European countries to combat global crimes, terrorism and deal with illegal immigration. It was then incorporated into a European Union law in 2008. It allows, in the European area, the automatic transmission of DNA traces and profiles of persons across the countries. The system is not yet fully operational, but many countries are already connected. The first results have been evaluated. Successful cases illustrate the value of the approach (Santos & Machado, 2017; Toom, 2018).

The process seems, however, much more difficult to implement than expected. Many disparities in the way processes are implemented in countries have also been highlighted. A trend emerges, indicating that only a very small part of matches obtained at an international level is finally integrated into a criminal procedure (Toom, 2018). This is due to their high number, difficulties of prosecuting internationally, as well as the definition of matches that creates significant probabilities of false positives. Scientists from traditional forensic science laboratories, who are part of the process, seem to have, in certain conditions, even unilaterally decided to retain information, when the police operate the DNA database in the

[2] https://www.cps.gov.uk/legal-guidance/streamlined-forensic-reporting-guidance-and-toolkit (accessed 8th of February 2020)

demanding country (Santos & Machado, 2017). This attitude typically results from the current forensic debate on risks of miscarriage of justice.

Regardless of how the process is implemented, it shows absolutely no connection with policing models. "Efficiency" goes implicitly hand in hand with the increase in the number of international identifications and prosecutions. However, simple statistical assessments and current experience show again changes of scale: when the network will be fully operational, criminal justice systems, already saturated, can be expected to become totally overwhelmed and ineffective to absorb DNA matches at the international level.

Priorities are required and they must balance the particularities of the case against other policing strategy guiding how the infrastructure should be used. In particular, in a proactive policing model, the importance of relying on targeting high concentrations of crimes and finding patterns will increase. Linking crimes will therefore be considered of utmost importance to detect the most relevant repetitive problems, help decipher their structure and implement effective responses. If such a view is adopted, beyond the identification of people, the links between crime and DNA will be much more ambitiously integrated into the analysis of crime. This application is currently largely ignored. Another advantage is that (unidentified) profile links significantly reduce legal issues, compared to the direct cross-border transmission of information about individuals. Such an approach has been successfully tested regionally (Rossy, Ioset, Dessimoz, & Ribaux, 2013).

Other forensic transformations

DNA is only one example, but ongoing transformations underlying forensic technologies go well beyond this area. The control of individuals (*e.g.* identity checks, alcohol control by means of a breath analyzer, potentially illicit substances carried on by a person tested by NIR infrared tools and incoming Lab-on-Chip (LOC)) are also made much more immediate and easy to systematize in the field, blurring the previous investigative/evaluative dichotomy (Casey et al., 2019). Artificial intelligence systems eventually support decisions in the process, which go through the assessment of the risk presented by individuals, aspects of predictive policing or even lead to the implementation of so-called predictive justice (Nissan, 2017). Some of these technologies are only at the level of basic research, and the promises are sometimes higher than what they can actually deliver, while others are fully operational.

Regardless of the state of technology transfer in practice, the inclusion of powerful information processing in the criminal proceedings alters the scope and nature of surveillance, the rate of arrests, the detections of crimes or even the volume of punishment distributed. All these changes enhance the application of the traditional law enforcement paradigm on a scale that can create unintended and uncontrolled side-effects. For example, in addition to the many computerized biometric processes that have an impact on individual liberties, at another spectrum of the law enforcement model, automated license plate recognition changes the order of magnitude of those sanctioned for speeding or parking. It is impossible to predict how society in general will react to these changes, and what moral values will emerge from such transformations.

Eventually, some commentators even consider that prosecuting large-scale global cybercrimes in the traditional way is too difficult, if not impossible (Dupont, 2017). Crime statistics have recently highlighted the extent of cyber-victimization, as well as of their new pervasive forms such as online frauds (BCS, 2016). Police are changing their processes to integrate this new crime landscape and to develop the necessary investigative skills. There is, however, much hesitation about where to go from here (Rossy & Ribaux, 2020). It might be that the law enforcement reactive model, under its current traditions, will not resist to digital transformations.

The raise of the digital forensics community

The organizational movement to integrate computer specialists and new technical positions into police structures in the 1980s called for a change of police culture. This new digital forensics community has largely developed on the margins of the forensic and police professions (Pollitt, 2010). This community has gradually organized itself with rare academics to share knowledge and experiences. For a long time, this activity was carried out with relative indifference on the part of their organization. Digitalization created a radical change of scale in one of the most sensitive domain of crime investigation: pedophilia. This was one of the catalysts that led the police to examine the need to create an Internet investigative capacity within their own organization. At the same time, mobile phone data began to be used progressively in a more systematic way until the emergence of the smart phone around 2007. This created major changes, as this information has provided quick insight into the relations between entities (persons, phones), locations, and time, which are the main dimensions to exploit when investigating a crime. The flow of digital images to be processed has also increased considerably: it can be stated that, nowadays, each interesting event occurring in a public space is necessarily filmed, providing a new stream of traces to collect and exploit.

The activity of specialists extracting information from the device became more central and borderline between forensic science (how to extract and interpret data from multiple devices), the investigation (how to integrate this information with other sources of information) and criminal intelligence analysis (how to manage the large amount of information generated, how to structure knowledge around criminal networks). These changes impacted the traditional organization of investigations and underlies tensions in applying combinations of policing models (law enforcement and intelligence-led). This community has also created new fragmentations (new skill profiles, new units, new roles, new silos). At the same time, it is struggling to keep pace with the dynamics behind the evolution of technologies. It is finally under higher pressure because quality control of forensic processes is rather weak in a police context, while legal developments considerably reinforce respect for fundamental rights and fair justice.

The traditional forensic laboratory can difficultly accommodate the new digital community, since the separation with the police has been a strategic goal to achieve in order to avoid any kind of biases (underlined by the quality management solution to forensic science critics). This contradicts the fact that it is especially at the beginning of the investigations that digital information is quickly used to conduct inquiries, with a high level of integration. In this context, where dynamic interactions amongst the various stakeholders in the investigation are required, the services of an external laboratory are not easy to set up and formalize clearly. Digital investigations require also attendance to crime scenes, which was largely deserted by most centralized forensic science laboratories.

The, *de facto*, central role taken by this community in police organizations causes tensions and anomalies that call for very deep reconfigurations in terms of policing strategies, as well as of delineating roles and tasks, relations with other private/public stakeholders or with the public in general.

Synthesis: traceology at the core of proactive policing in the new age

As current digitalization exacerbates existing tensions between traditional law enforcement and proactive forms of policing, we postulate that simple application of usual law enforcement strategies will not work in the coming era of digital transformations: the systematic application of innovative identification techniques produces already new volume of matches and hits that neither the police, nor the justice systems are able to deal with. Cyber-crimes are global, requiring complex cross-jurisdictional investigations with low success rates; technologies are evolving at a high rate, making it impossible for organizations to keep pace and switch from one technology to another for conducting investigations. Hence, there is a trend to rely on the private sector, Big Tech and local IT providers, despite of all the organizational, economical and ethical problems ensuing. Investigations, in their current conception, are unlikely to succeed in the case of emerging so-called cyber-volume crimes (e.g. online fraud), which are ubiquitous, large-scale, etc.

Reforming policing models in the new context must consider the fact that everything changes in scale. Of particular importance is the volume and variety of traces generated by human and illicit activities, as well as the many methods and tools available to detect, collect and analyze them. One priority is therefore to create a framework for using these ubiquitous and basic pieces of information. Boullier (2017) considers traces as the atomic form of information for studying sociological, and hence criminological, phenomena in the digital age. The trace is, however, created on physical and computer substrates. It entirely depends on the immediate environment in which the activities of interest take place. Interpreting out of norms human activities through traces is exactly what forensic science is about (Margot, 2011). The term of traceology is increasingly used instead. This is to disconnect forensic science from its law enforcement connotation, and suggest a broader view (Margot, 2011). Whatever the terminology, a science of the trace has a pivotal role to play. A lot of basic principles, methods and tools elaborated in forensic science can serve as a fundamental framework. Adopting this view requires, however, mutations of the discipline and a more ambitious vision connected with policing aims: forensic science has to go beyond its well-established position as a service provider for the criminal justice system in a law enforcement perspective.

At its very bottom, the forensic science community should first integrate its different pieces. The digital forensics community has evolved until now too independently from the field of forensic science for supporting this vision. This is changing by a cross fertilization movement, where the terms have been redefined and cover a broader and integrative view on the forensic contribution (Pollitt, Casey, Jaquet-Chiffelle, & Gladyshev, 2018). This is a step towards the creation in professional practices of an homogenous forensic ecosystem that makes the best use and account of the information available along evaluative, investigative, and intelligence processes (Casey, 2019). This ecosystem must incorporate models of knowledge management and dissemination that adapt to the pace of change, the legal environment and the fact that highly specialized technologies tend to become commonplace rapidly. The sharing and reuse of experience through case-based reasoning and collaborative platforms complement this first proposal (Baechler et al., 2020; Casey, 2019).

On top of these bases, traces should be more actively and ambitiously integrated into crime analysis and forensic intelligence models for serving proactive policing models (Casey, 2019). There are many dimensions to explore, such as how traces can support the search for crime concentrations in new topological spaces and timescale, or how they help decipher the anatomy of certain frauds. This is accompanied by considerations about the nature of social interactions in virtual spaces and about new forms of organizations and implementation of crime processes, which generate traces in the form of patterns to be found (Dupont, 2017; Leukfeldt, Kleemans, & Stol, 2017).

This new forensic and crime analysis framework would then integrate knowledge brought by a new wave of research works around pervasive crime mechanisms of the digital age that together depend on communication infrastructures and have a strong physical component (Leukfeldt et al., 2017; Pazos, Giannasi, Rossy, & Esseiva, 2013; Rossy & Ribaux, 2020).

This new paradigm, based on the trace and taking into account policing experience and knowledge, integrates most of the cybersecurity concerns such as incident detection, incident response and forensic preparedness, infrastructure resilience, surveillance, protection and prevention (CMM, 2016). It brings much more by incorporating the many years of forensic, police and criminological experience that are poorly reflected in cybersecurity models. This joint effort will help draw the lines of a comprehensive model of policing in the digital age.

Conclusion

Digital transformations are requiring in-depth reforms in policing. The latter is currently shaken by the arrival of a new community of specialists that has grown-up in relation to digitalization. It was, at first sight, supposed to deliver only technological services, and supporting traditional activities. However, this minimalist conception is not sustainable, as scales in human traceability and of crimes in many forms have changed dramatically, requiring new approaches to forensic science, investigation, crime analysis, intelligence and policing.

Elemental forensic science, or traceology, as well as theories behind proactive policing models consist of solid basis on which to build new frameworks. This requires that borders between the police professions and other stakeholders must be reshaped in a very ambitious and determined way. There is, however, still significant efforts to deploy so that managers and key decision-makers realize this potential (see also chapter 9 – Crispino et al.).

Bibliography

Baechler, S., Morelato, M., Gittelson, S., Walsh, S., Margot, P., Roux, C., & Ribaux, O. (2020). Breaking the barriers between intelligence, investigation and evaluation: a continuous approach to define the contribution and scope of forensic science. *Forensic science international*, 110213. doi:10.1016/j.forsciint.2020.110213

BCS. (2016). *Crime in England and Wales-Year ending March 2016*: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingmarch2016.

Bieber, F. R. (2006). Turning Base Hits into Earned Runs: Improving the Effectiveness of Forensic DNA Data Bank Programs. *The Journal of Law, Medicine & Ethics, 34*(2), 222-233. doi:10.1111/j.1748-720X.2006.00029.x

Bieber, F. R., Brenner, C. H., & Lazer, D. (2006). Finding Criminals Through DNA of Their Relatives. *Science, 312*(5778), 1315-1316.

Bitzer, S., Delémont, O., & Ribaux, O. (2016). To analyse a trace or not? Evaluating the decision-making process in the criminal investigation. *Forensic science international, 262*, 1-10.

Boullier, D. (2017). Big data challenge for social sciences and market research: from society and opinion to replication. In F. Cochoy, J. Hagberg, M. Petersson McIntyre, & N. Sörum (Eds.), *Digitalizing Consumption, Tracing How Devices Shape Consumer Culture*. London and New York: Routeledge.

Bradbury, S.-A., & Feist, A. (2005). *The Use of Forensic Science in Volume Crime Investigations: a Review of the Research Literature* (43/05). Home Office, Londres.

Brown, C., & Ross, A. (2012). *End-To-End Forensic Identification Process Project. Volume Crime*. Australia New Zealand Policing Advisory Agency - National Institute of Forensic Science.

Casey, E. (2019). The Checkered Past and Risky Future of Digital Forensics. *Autralian Journal of Forensic Sciences, 51*(6), 649-664. doi:10.1080/00450618.2018.1554090

Casey, E., Ribaux, O., & Roux, C. (2019). The Kodak syndrome: risks and opportunities created by decentralization of forensic capabilities. *Journal of Forensic Sciences, 64*(1), 127-136. doi:10.1111/1556-4029.13849

Castella, V., & Mangin, P. (2008). DNA profiling success and relevance of 1739 contact stains from caseworks. *Forensic Science International: Genetics 1*(1), 405-407. .

CMM. (2016). *Cybersecurity Capacity Maturity Model for Nations (CMM)*. Global Cyber Security Capacity Centre, University of Oxford, Oxford.

Dupont, B. (2017). Bots, cops, and corporations: on the limits of enforcement and the promise of polycentric regulation as a way to control large-scale cybercrime. *Crime, Law and Social Change, 67*(1), 97-116. doi:10.1007/s10611-016-9649-z

Erlich, Y., Shor, T., Pe'er, I., & Carmi, S. (2018). Identity inference of genomic data using long-range familial searches. *Science, 362*(6415), 690-694.

Keay, S., & Kirby, S. (2018). The Evolution of the Police Analyst and the Influence of Evidence-Based Policing. *Policing: A Journal of Policy and Practice, 12*(3), 265-276. doi:10.1093/police/pax065

Leukfeldt, E. R., Kleemans, E. R., & Stol, W. P. (2017). Cybercriminal Networks, Social Ties and Online Forums: Social Ties Versus Digital Ties Within Phishing and Malware Networks. *The British Journal of Criminology, 57*(3), 704-722. doi:10.1093/bjc/azw009

Maguire, C. N., McCallum, L. A., Storey, C., & Whitaker, J. P. (2014). Familial Searching: A Specialist Forensic DNA Profiling Service Utilising the National DNA Database® to Identify Unknown Offenders via Their Relatives - The UK Experience. *Forensic Science International: Genetics, 8*(1), 1-9.

Margot, P. (2011). Commentary on the Need for a Research Culture in the Forensic Sciences. *UCLA Law Review, 58*(3), 795-801.

Mc Cartney, C. (2006). *Forensic Identification and Criminal Justice*: Willan.

Mc Cartney, C. (2019). Streamlined forensic reporting: Rhetoric and reality. *Forensic Science International: Synergy, 1*, 83-85.

NAS. (2009). *Strengthening Forensic Science in the United States: a Path Forward*. National Research Council of the National Academies, Washington D.C.

Nissan, E. (2017). Digital technologies and artificial intelligence's present and foreseeable impact on lawyering, judging, policing and law enforcement. *AI & SOCIETY, 32*(3), 441-464. doi:10.1007/s00146-015-0596-5

Pazos, D., Giannasi, P., Rossy, Q., & Esseiva, P. (2013). Combining Internet Monitoring Processes, Packaging and Isotopic Analyses to Determine The Market Structure: The Example of Gamma Butyrolactone. *Forensic science international, 230*(1-3), 29-36.

PCAST. (2016). *Forensic Science in Criminal Courts: Ensuring Scientific Validity of Feature-Comparison Methods*. Executive Office of the President President's Council of Advisors on Science and Technology Committee, Washington.

Pham ‐ Hoai, E., Crispino, F., & Hampikian, G. (2014). The First Successful Use of a Low Stringency Familial Match in a French Criminal Investigation. *Journal of Forensic Sciences, 9*(3). Retrieved from 10.1111/1556-4029.12372

Pollitt, M. (2010, 2010//). *A History of Digital Forensics.* Paper presented at the Advances in Digital Forensics VI, Berlin, Heidelberg.

Pollitt, M., Casey, E., Jaquet-Chiffelle, D.-O., & Gladyshev, P. (2018). *A Framework for Harmonizing Forensic Science Practices and Digital/Multimedia Evidence*. OSAC Task Group on Digital/Multimedia Science.

Ratcliffe, J. (2016). *Intelligence-Led Policing* (2nd edition ed.). Cullompton, UK: Willan.

Rossy, Q., Ioset, S., Dessimoz, D., & Ribaux, O. (2013). Integrating forensic information in a crime intelligence database. *Forensic science international, 230*, 137-146. doi:10.1016/j.forsciint.2012.10.010

Rossy, Q., & Ribaux, O. (2020). Orienting the Development of Crime Analysis Processes in Police Organisations Covering the Digital Transformations of Fraud Mechanisms. *European Journal on Criminal Policy and Research*. doi:10.1007/s10610-020-09438-3

Roux, C., Talbot-Wright, B., Robertson, J., Crispino, F., & Ribaux, O. (2015). *The end of the (forensic science) world as we know it? The example of trace evidence* (Vol. 370).

Santos, F., & Machado, H. (2017). Patterns of exchange of forensic DNA data in the European Union through the Prüm system. *Science and Justice, 57*, 307–313.

Scudder, N., Robertson, J., Kelty, S. F., Walsh, S. J., & McNevin, D. (2018). Crowdsourced and crowdfunded: the future of forensic DNA? *Australian Journal of Forensic Sciences*, 1-7. doi:10.1080/00450618.2018.1486456

Strom, K. J., & Hickman, M. J. (2010). Unanalyzed Evidence in Law Enforcement Agencies. *Criminology & Public Policy, 9*, 381-404.

Tilley, N., & Ford, A. (1996). *Forensic Science and Crime Investigation* (73). Police Research Group, Home office, London.

Toom, V. (2018). *Cross-border exchanges and Comparison of Forensic DNA data in the context of the Prüm Decision*. Policy Department for Citizens' Rights and Constitutional Affairs, European Parliament, Bruxelles.

Vincent, F. (2010). *Inquiry into the Circumstances that Led to the Convicition of Mr. Farah Abdulkadir Jama* (PP no. 301, Session 2006-10). Victorian Government, Melbourne.

Weisburd, D., & Majmundar, M. K. (2018). *Proactive Policing. Effects on Crime and Communities (2018)*. National Academies of Sciences, Engineering, and Medicine, Division of Behavioral and Social Sciences and Education; Committee on Law and Justice; Committee on Proactive Policing: Effects on Crime, Communities, and Civil Liberties.

Weisburd, D., & Neyroud, P. (2013). *Police Science: Toward a New Paradigm*. National Institute of Justice.

Zedner, L. (2007). Pre-crime and post-criminology? *Theoretical Criminology, 11*(2), 261-281.