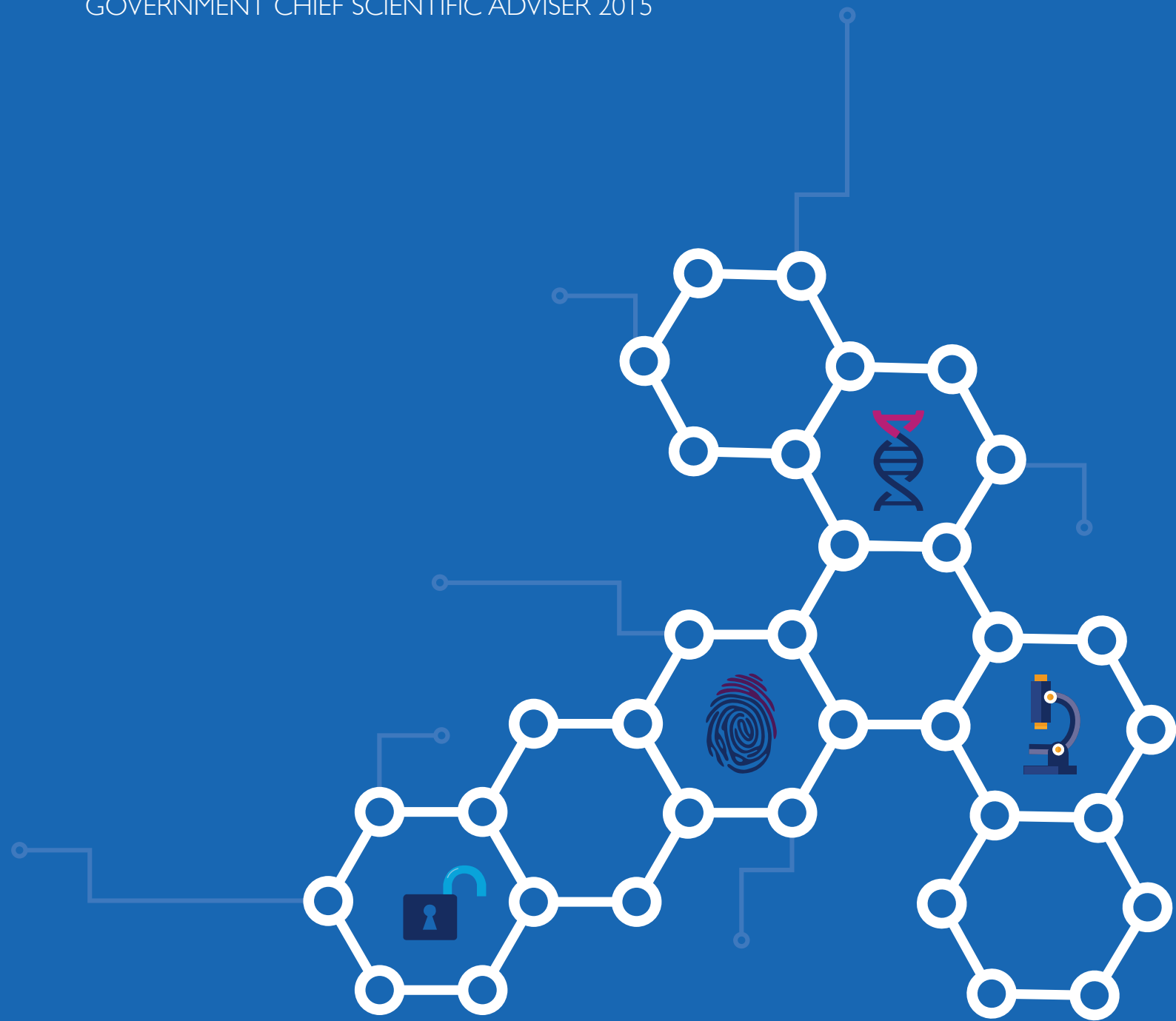
Government
Office for Science

FORENSIC SCIENCE AND BEYOND: AUTHENTICITY, PROVENANCE AND ASSURANCE

ANNUAL REPORT OF THE
GOVERNMENT CHIEF SCIENTIFIC ADVISER 2015



Forensic Science and Beyond: Authenticity, Provenance and Assurance
This is the second Annual Report of the Government Chief Scientific Adviser, Sir Mark Walport

Editor: *Mark Peplow*

Authors: *Sir Mark Walport, Government Chief Scientific Adviser; Claire Craig, Director, Government Office for Science; Elizabeth Surkovic, Deputy Director, Government Office for Science*

This report is intended for:
Policymakers, legislators, and a wide range of business people, professionals, researchers and other individuals whose interests include the use of forensic analysis within the Criminal Justice System through to authenticity, provenance and assurance in the provision of goods and services.

This report should be cited as:
Annual Report of the Government Chief Scientific Adviser 2015. Forensic Science and Beyond: Authenticity, Provenance and Assurance. The Government Office for Science, London

The Government Office for Science would like to thank the authors who contributed chapters, case studies and their time towards this report and gave it freely. A full list of authors can be found in the companion document: Forensic Science and Beyond: Authenticity, Provenance and Assurance. Evidence and Case Studies.

The report project team was Martin Glasspool, Richard Meadows, Lindsay Taylor, Adam Trigg and Jenny Wooldridge.

This report is presented in two parts. The first is the summary report of the Government Chief Scientific Adviser. This was developed as a result of seminars and the advice of the experts who provided the source of the evidence. The second part, the evidence, has been gathered from and written by a distinguished group of experts. The evidence takes two forms: chapters that consider a major aspect of the forensic landscape; and individual case studies that illuminate points of detail and principle. The evidence section provides the views of the experts themselves, who met on several occasions during the preparation of the report and had the opportunity to help to develop the narrative and to comment on each other's contributions. The Government Chief Scientific Adviser is responsible and accountable for the summary report, and the experts for their individual contributions to the evidence papers and case studies. Neither should be blamed for the sins and omissions of the other!

FOREWORD

Security, productivity and innovation are at the heart of this Government's agenda. In this report "Forensic Science and Beyond: Authenticity, Provenance and Assurance", Professor Sir Mark Walport, the Government's Chief Scientific Adviser, explores the use of innovative analytical techniques, both now and in the future. The report considers how forensic analysis, in its many forms, can be applied more effectively to assure us of the provenance and authenticity of the goods and services that we buy and use. If the power of these techniques can be unlocked, that will lead to a further increase in productivity in the UK economy, making markets more trustworthy and creating new forms of added value for innovative businesses to capture.

Inevitably, in a report of this name, the realm of the criminal justice system looms large. Here, rather than look at operational detail, the report explores broader issues such as language, ethics and the use of forensics to predict crime and importantly, to prevent crime from occurring in the first place. The thoughtful challenges presented in this report are addressed to policy makers across Government and also to the private sector. I commend it to both.

Oliver Letwin,
Chancellor of the Duchy of Lancaster

FORENSIC SCIENCE AND BEYOND: AUTHENTICITY, PROVENANCE AND ASSURANCE

Sir Mark Walport,
Government Chief Scientific Adviser

WHY A REPORT ABOUT FORENSICS?

This report is about the power of analytical science and its many applications. It starts with forensics – the use of analytical science to assist the courts with issues such as identity and identification. But the power of forensic analysis has the ability to deliver benefits to society that go far beyond the Criminal Justice System. This report explores the many ways in which we can use analytical scientific tools, combined with the approaches and skills of the forensic scientist, to reap the rewards of these benefits.

Why produce a report about forensic science and its broad applications now? The majority of the advice to the government from the Government Chief Scientific Adviser falls into three domains. These are:

1. the identification of emerging technology and advice on how government can derive greatest benefit for the economy, policymaking and delivery of government services;
2. the provision of evidence supporting the development of government policy; and
3. support for national resilience and security.

Forensic science is an apt topic for advice as it is important to all three of these domains. A series of emerging technologies are coalescing to power major advances in the analytical sciences that underpin forensic science. These include genomic science, information technology, machine intelligence, the internet of things, and quantum technologies. And these emerging technologies themselves create new domains for forensic analysis.

In today's world, cyberspace may be viewed as the most important focus amongst these new domains. This is a new and rapidly-developing global infrastructure, engineered entirely by humans and only partially governed by national governments, on which we are now almost completely dependent. In cyberspace, people have opportunities to create new identities, conceal themselves and act across national boundaries and commit crimes that could not have been envisaged in the past.

Government needs evidence on what forensic approaches can and cannot achieve realistically, and what are the uncertainties about the best uses of forensics now and in the future. So evidence about forensics is vital to make robust policies in areas ranging from the justice system to the financial services sector. It is needed by agencies ranging from the security services to the Food Standards Agency; by the Department of Health and the NHS, which must provide assurance that the medicines we take are not substandard or counterfeit; and by the Bank of England, to ensure that our banknotes are not forged and to explore possible roles for digital currencies. All free markets depend on the existence of trustworthy systems for the provision of goods and services, and secure authentication of both buyers and sellers.

Our resilience depends on the quality of our infrastructure. This falls into three categories. The first is our human built, engineered, manufactured and technological infrastructure. The second is our natural infrastructure, comprising human, animal and plant health, and our geophysical environment including water, weather and climate. The third is our social infrastructure, of family, friends and communities, including the social infrastructure of the nation state. This social infrastructure is shaped by the physical organisation of our countries, cities, towns and villages and is now also virtually located in cyberspace, linked by social media and search engines. Forensic analysis is crucial to understanding all types of infrastructure and our interactions with it.

This, my second annual report, provides evidence to policymakers that will enable them to decide what actions to take to maximise the benefits for the UK from the emerging analytical techniques that power forensic analysis. Achieving these benefits will depend not only on our

mastery of the tools themselves but also on a supply of people with the right spectrum of skills. It will require close collaboration between a range of scientific disciplines, entrepreneurs and regulators. Importantly it will require strong public engagement leading to robust democratic decisions about the circumstances – the where, when and how – in which these powerful tools will be employed.

In the spirit of providing advice rather than advocating policy, the recommendations are framed as questions that point to the key areas where policymakers need to decide whether and how to act. For these purposes, the policy community includes government, its agencies, and the analytical and forensic professions themselves.

AN OVERVIEW OF THE OPPORTUNITIES AND CHALLENGES FOR FORENSICS

Today's scientific advances mean that we can measure and detect tiny traces of substances with great accuracy and precision. The underlying analytical science has vastly improved our ability to solve and to prevent crime through their application in forensic science. They also create wholly new opportunities and challenges for both science and society. The potential applications of forensic science go much further than investigating and solving crime. As Gary Pugh says in Chapter 2: "The practice of forensic science is one of the most widely known and least understood areas of scientific endeavour".

Wherever we go and whatever we do, we leave traces of our presence. These may be physical traces, such as DNA, or traces of our microbiomes – the collection of bacteria and other micro-organisms that colonise our skin, our mouths and nasal passages, and our guts. They may be virtual traces, such as digital records of financial transactions. A range of very different technologies enables us to learn much more from an object, sample or set of data than ever before. We can detect and identify diminishingly small amounts of physical and biological material, and are increasingly able to gather and interrogate ever enlarging data sets.

Meanwhile, the application of widespread and embedded information technologies means that our actions may leave new types of traces in virtual spaces. These virtual spaces place a large and increasing strain on the supply of skills and tools needed to conduct forensic investigations. They also give rise to the challenge of how to apply forensic techniques in these new globally-distributed and potentially 'ungoverned' spaces such as the Dark Web. Increasingly there is a blurring of the digital and physical world. For instance, some printers deposit almost invisible tracking codes allowing the printed document to be traced back to the printer; digital cameras act similarly.

The term 'forensic' once meant 'relating to courts of law', but increasingly is being used to mean the practice of meticulous examination and careful focus on details in any sphere of activity. The potential to know more about the world in this way creates many opportunities. Used properly, it can help reduce crime and assure the quality and origin of goods and services, creating new markets.

Because forensic science enables new forms of assurance and can increase confidence about the provenance of objects, it opens up possibilities for the better design of systems that promote growth and ensure security. It provides new methods for designing out crime before it happens: for example, pre-emptively deterring cybercrime and financial fraud, or constraining the markets for counterfeit pharmaceuticals and other goods. These are the future equivalents of designing the milled

edges to silver coins that stopped them being 'clipped' by criminals. These aspects are explored in Section 2 of the report and provide rich material for innovation in crime prevention.

New capabilities create other challenges for our existing systems; in particular, our ability to analyse may outstrip our ability to interpret. Because we can identify very small traces of a substance, we need greater certainty in understanding their significance and better ways to communicate different levels of confidence. In her case study on p120 of Chapter 10, Francesca Bray explores how, applied to the messiness of the real world, these capabilities can ultimately challenge our notion of purity. They expose that almost nothing is 'pure' and show how little we know about the composition of substances present at very low concentrations in the air, water or land around us.

An analysis of a humble glass of water will find that it contains far more than just H_2O. More often than not the scientist recognises that the levels of background chemicals in tap water or in a bottle of mineral water are so low that they can have little consequence for the health of the consumer. However the large market in bottled waters, which may claim benefits to the consumer from their 'purity' or mineral content, shows that many people have beliefs and values that ignore the scientific perspective.

The job of the scientific adviser is clear: it is to provide the best evidence on objective measures of benefit or harm to health relating to the purity of the air we breathe, the water we drink, or the food that we eat. Providing and communicating such evidence enables better-informed debate to help decision-makers, who look through the lenses of science and of human values to make their decisions. These topics were the main focus of my 2014 Annual Report on innovation and risk.

FORENSIC SCIENCE IN THE CRIMINAL JUSTICE SYSTEM

The first key message to policymakers is that, while forensic evidence has a vital role to play within the courtroom, its role within the Criminal Justice System goes far beyond, and even before, the courts themselves. And beyond the Criminal Justice System, forensic techniques underpin essential work in establishing provenance and authenticity and giving assurance in areas such as environmental protection, food and drink, pharmaceuticals and consumer products.

There is a long journey from the collection of traces at a crime scene to the use of these as evidence in a courtroom, described by Karen Squibb-Williams and Angela Gallop in Chapter 1. The use of forensics in the Criminal Justice System starts with those who collect the traces that have the potential to become evidence. It proceeds to those who analyse these traces and present the results to others who must decide on its usefulness as evidence. These users are the police and other law enforcement agencies, and those, such as the Crown Prosecution Service, who must decide whether to prosecute. Finally forensic science reaches the courts, comprising the plaintiffs, judges, lawyers and jurors, who must be able to understand the weight of the forensic evidence in the context of all the other evidence presented. There is anecdotal evidence (see Chapter 1) that only a small proportion of cases involving forensic science evidence reach a courtroom, and we need to understand better why there is such a high attrition rate. This could be for several reasons. It could signal a lack of confidence in forensic techniques or results to achieve justice in the courtroom. Alternatively the use of forensics may exclude guilt or facilitate a guilty plea, avoiding the need for an adversarial courtroom appearance, as described in the Chapter 15 case study (see p172) on indecent image detection. It may simply be that the forensic analysis was inconclusive. Whatever the reasons, any analysis of the effectiveness of the use of forensics in the justice system must take a system-wide approach and not focus solely on the courts.

The second key message is that the complexity of forensic evidence is increasing rapidly, and policymakers and practitioners will need to adapt and innovate in response. It is increasing in three ways. Firstly, the 'classical' forensic evidence that links a person to a place,

or an event, is becoming more sophisticated and has the potential to become even more so, for example through the traces we leave with GPS tracking on our mobile phones or devices connected to the internet. Secondly, there are whole new classes of forensic evidence relating to the new infrastructures for crime in cyberspace and across national boundaries, such as IP address tracing. Thirdly, there are new types of forensic evidence relating to the tools and the objects used to deter crime, such as the widespread use of radio-frequency identification (RFID) tagging and new techniques for 'watermarking' physical and digital assets.

In addition, the unprecedented sensitivity of new detection methods, be it from amplification of traces of DNA or the ability to measure minute chemical signatures, raises important questions about distinguishing the 'signal' from the background 'noise'. When is a positive or a negative result 'true' or 'false'? The result itself needs to be considered in the context of the ascertainment of the sample. Where did it come from? What was sampled and what was not? What were the standards against which the analysis was performed? As Itiel Dror describes in Chapter 4, there is potential for cognitive biases to affect many stages of the forensic analysis. This is because human brains do not really 'see' the world as it is, but adopt many essential short cuts to get to what is usually the most important information. He outlines ways to improve analysis, including training forensic scientists, judges, lawyers and jurors to be aware of the nature of cognitive biases, which will itself help to counteract them.

The experts providing evidence for this report took a consistent view that the different actors in the criminal justice system are hampered by differences in terms and language to describe the meaning and significance of forensic evidence, and the measures of uncertainty associated with it. **The third key message** is that all participants across forensic science need to overcome the challenges associated with communication, consistency, collaboration, clarity and common standards. At each stage of the decision-making process along the chain of justice, how can 'uncertainty' be expressed in a language that is agreed by all parties? Uncertainty is usually on an analogue, not a binary scale – so how should it be quantified, and how does uncertainty from a 'scientific' test fit into the panoply of other uncertainties in reaching the best outcome for all of the participants in the justice system?

None of this undermines the power of forensic analysis: fingerprinting and DNA analysis have transformed the determination of serious crimes from rape to murder. But forensic analysis could offer even more. Itiel Dror highlights the need to address cognitive issues and the need for standardisation, using fingerprint analysis as an example. Errors in evaluation of forensic evidence and variation in forensic decision making do occur, but robust standards of application and subsequent interpretation, together with the right kinds of investments in skills and techniques, as well as regulation, will ensure better outcomes for society as the technologies evolve.

Josephine Bunch (Chapter 3) outlines recent improvements to the forensic quality system in the UK, and the need to continue to increase confidence in the adherence to standards by national and international players. The Forensic Science Regulator's office, through its Codes of Practice and Conduct, identified accreditation as the means to demonstrate appropriate quality standards. The next generation of forensic scientists also needs to be prepared to meet the challenges of the changing nature of the discipline, and the Chartered Society of Forensic Sciences has a key role through its accreditation of universities' forensic science courses.

However, the evidence presents a consistent view that there are barriers between the different actors in the justice system, caused by their differing language and communication about the meaning and significance of forensic evidence, and of the measures of uncertainty associated with different types of result.

The questions to policymakers are:

Q What forum should provide the opportunity for discussions between the different participants in the justice system about the nature and significance of the applications and interpretation of forensic approaches and tests?

Q How should information – especially the measurement and communication of the inevitable uncertainties – be provided initially to the prosecutors or lawyers, then to a court in a manner that is clear and understandable to all participants in the legal process?

Q How could a forum be set up in a fashion that would enable it to undertake horizon scanning and respond to new and emerging tests and approaches?

Q What are the best pathways from discussion to implementation and practice?

THE DOMAIN OF CYBERSPACE

The fastest growing domain of criminality is cyberspace. The global nature and relative anonymity of digital transactions, aided in part by tools and services available on the Dark Web, has enabled the creation of a global supply chain of tools, information, data and products. These enable such crimes as the sharing of indecent images of children, information and financial theft, identity theft, the development of malware, virus creation and malicious hacking. These new forms of crime, and possible means to combat them, are discussed by Andrew Blyth and Matt Johnson in Chapter 7. Because the perpetrators of these crimes and their victims live in the physical world, there is almost invariably an interface between bytes and humans that provides both a threat and an opportunity.

Vulnerabilities are caused by deficiencies in computer code, but also by deficient computer hardware and networks. Humans often provide the weakest link, and are the hardest to 'patch', or correct. They can act as insiders, implementing flawed software solutions or compromising the integrity of computer systems; or be exploited by outside users, as poor custodians of their passwords or by falling prey to phishing attacks and other fraudulent approaches.

A key question for anyone seeking services and products via the internet is: "Can I trust the person or organisation that I am interacting with?". To answer that question I need to know two things: first, that you are who you say you are (authentication); and second, that you have the necessary permission to do as you claim (authorisation).

We need to understand the vulnerabilities and threats in order to put in place the best risk management strategies. Risk management requires people to 'own' the risk, along with the necessary toolkit to prevent risks from transpiring, to mitigate their consequences, to handle them in the event that they occur, and to clear up afterwards.

A high degree of expertise is needed for the risk owners in the digital universe, because the digital implementations are so highly technical. In the digital world the key toolkit comprises three highly important sets of code: one for government, the second for the implementers and providers of digital services and products, and the third for all parties in the enterprise. Governments control the traditional code of law, underpinned by legislation and regulation. The implementers and providers of the services and products control the second, which is the code written by computer scientists. Governments working with the implementers and providers collectively control the third set of codes. These are the standards, typically international in their reach, that provide a framework of quality assurance that risk managers and customers for products and services can use as accountability measures for the providers. It is essential to focus on all of these to promote the development of reliable and secure digital services and products.

There are several challenges for forensic computer science. The first is a skills shortage. Rapidly enlarging markets for digital goods and service provision provide fertile territory for cybercrime, increasing the demand for computer forensic technologists. The second is the global nature of cybercrime, which demands global collaborations to enable the investigation and prosecution of perpetrators. The third is the sheer scale of digital forensic investigations, coupled with encryption of data and opportunities to erase or damage digital evidence. The fourth challenge is the interface between digital information and physical information, which may require collaboration between different types of experts. The fifth challenge is the challenge of communicating this highly technical information throughout the justice process.

There are also important opportunities. Objects translated from the digital to the physical can be 'watermarked' by almost invisible techniques, linking a page to a unique printer, or a photo to a unique camera. Sophisticated tracking of an intrusion through data logs can identify the origin of a hacking incident, and the case study on p73 of Chapter 6 by Lucina Hackman and colleagues provides examples of how digital images can be used to provide the physical identification of perpetrators, for instance through the anatomical features of a hand present in indecent images of children.

A key opportunity in the digital environment is to create, encourage and enforce the use of much more powerful and robust identity-management tools that provide authentication while protecting privacy. Distributed ledger technologies provide one example of a solution that could increase the assurance and robustness of a wide range of services. Distributed ledgers were first implemented widely using block chain algorithms, the underpinning technology for the cryptocurrency Bitcoin. A key enabler for digital currencies is a ledger that can record transactions of virtual cash.

Bitcoin transactions are recorded as blocks in the ledger, which are 'chained' together by solution of a cryptographic puzzle – hence the name block chain, for the computer algorithms underpinning the Bitcoin ledger, and cryptocurrency. All participants in Bitcoin have access to the same ledger – hence it is a 'distributed' ledger – and legitimate changes in one copy are reflected virtually immediately in all copies of the ledger. The paradox of Bitcoin is that, like physical cash, it can be used for illegal purposes; but unlike physical cash, there is a highly secure ledger that records all Bitcoin transfers, though not the purpose of those transfers. The opportunity is to develop software implementations similar to a block chain that provide highly sophisticated distributed ledgers with additional tools that can deter and prevent criminal activity. These opportunities have been considered in detail in the report on Distributed Ledger Technologies from the Government Office for Science, which provided eight recommendations to maximise the benefits and minimise the risks of these important and disruptive technological innovations.

The questions to policymakers are:

Q How can we ensure that the most effective identification and authentication protocols can be implemented for individuals and for organisations? Given the global nature of the internet, international standards will need to be considered as part of the answer and their development may provide opportunities to increase the competitiveness of British businesses.

Q How can we ensure that we have a sufficient body of highly skilled people, able to stay at the forefront of available digital forensic techniques?

Q How can all partners in the Criminal Justice System ensure that digitally based evidence can be used effectively and robustly?

THE PREVENTION OF CRIME

As Nick Ross sets out in Chapter 9, forensic science is not only about criminal justice. It also has a major part to play in preventing crime from happening in the first place. In the same way that milling the edge of coins and the machine engraving of banknotes has inhibited forgers since the 17th century, so modern technology can be used to deter, foil and inhibit the contemporary forger or other criminals.

Forensic analysis has helped to reduce burglary, violent crimes and fraud in the past by enabling us to understand how particular types of crime were committed, and by making the crime less attractive to the criminal. For example, the great reductions in car and phone theft have been largely delivered by designing systems that made detection more likely and the object less valuable when stolen. The coming challenge is to identify early markers for temptation that can lead to illegal activity, and then to find ways to design out the crime before it occurs. This is no 'Minority Report' scenario, attempting to identify specific individuals about to commit specific crimes, but a very straightforward use of inducements to civil behaviour.

For those with criminal intent, new tools for copying and imitation are extremely powerful and becoming more widely available, whether the product is printed, digital or three-dimensional. Bits and bytes can be copied with precise accuracy. The

supply chains for goods and services are increasingly multinational, creating further opportunities for criminal manipulation. And there are completely new targets for the forger, including the identities that humans adopt in our increasing use of the internet.

The question to policymakers is:

Q What more could be done to use forensic approaches to design out crime, including using the full range of established and emerging technologies?

DILEMMAS POSED BY NOVEL TECHNIQUES

Issues of identity and identification are not new, and the application of science to them has always been both fluid and contested. Fingerprinting emerged in India and China over 2000 years ago as a tool to identify workers and craftsmen. Biometric technologies such as facial recognition – notably as developed by Alphonse Bertillon – and graphology began to be used in the latter part of the 19th century. Fingerprints then became a prime identification tool at the start of the 20th century, after skirmishes over facial recognition techniques and the abuse of graphology meant that both of those tools were discredited.

We continue to use human skills of facial recognition in the 'identity parade' and are now developing algorithms that can support human judgement. Accurate facial recognition by software 'in the field' remains difficult, but can be achieved reliably in situations where the facial position and lighting can be controlled.

The work of Alec Jeffreys in the latter part of the 20th century brought DNA identification to the fore. At present, DNA variation is essentially used as a 'barcode' that can be linked to the identity of an individual, but DNA sequencing has the potential to offer much more. Sequences can provide information about the characteristics of an individual such as whether they are genetically female or male, or the natural colour of their hair. It can provide information about the relatedness of one individual to others, and provide some information on ancestral origin. The sequence of a Y chromosome can, in certain circumstances, suggest a possible surname of a male (since males inherit both their Y chromosome and typically their surname from their fathers).

How these techniques might be developed and used in the future must be debated. As we said in last year's Annual Report: "We can only have the best discussion about innovations if we understand that the discussion must be about both science and values. There are some areas of technology and innovation that trigger particularly strong and immediate value-based responses, and these typically vary between different communities and countries". In that report, we went on to explore the need for good governance models, this being particularly important when dealing with our most personal information. "Most of us have neither the time nor the expertise to examine every decision or explore all the evidence. We rely on judgements about the values and behaviours of those in charge. For the individual, 'critical trust' may be the best frame of mind: neither outright scepticism nor uncritical acceptance."

The questions to policymakers are:

Q How can we best support the effective use of emerging forensic techniques and ensure the public remains confident in them?

Q What is the reliability of our measurement techniques, both the detection of false positive and false negative results, and how can the reliability be increased?

Q Considering specific technologies for specific purposes: what are the acceptable boundaries for the use and interpretation of forensic evidence?

Q Where might it be acceptable to use DNA to provide phenotypic and physical characteristics of an individual?

Q Where DNA technology is being used, what are the necessary standards and accreditation mechanisms for analysis and interpretation?

Q Do we need a new forum to debate and deliberate on the scientific and ethical issues relating to forensic techniques and perhaps to oversee and regulate their application?

ASSURING IDENTITY AND PROVENANCE

Trustworthy markets depend on us as customers being able to answer three questions. How do we know that an object is what it is claimed to be? How can we assure ourselves of the provenance of that object? And how can we assure the identity of the individual or organisation that provides the goods and services? Forensic approaches can help answer all of these questions.

Before setting out how technologies may help to assure our goods and services – a topic covered in Chapter 13 – we should acknowledge some of the reasons why new solutions may not be implemented as fast or as effectively as might be desired.

In principle, the interests of those that provide legitimate goods and services and those that purchase them should be completely aligned. But life is not so simple, and there are disincentives to both suppliers and consumers to maximising the uptake of technology to reduce crime and bad practices.

On the supply side, there are both direct and opportunity costs to suppliers in assuring the supply chain and identity for their goods and services. Tracing a garment from the cotton field or acrylic factory to the shop involves many steps, and the financial margins at some of these steps may be extremely small. The same applies to very many products, from foods to high tech products. Suppliers are also highly protective of the brand of their products– and it can be damaging to the brand if it transpires that the producer's supply chain has been contaminated with counterfeit or substandard components or products – so there may be a disincentive to 'owning up'.

On the consumer side, there are incentives for customers to turn a 'blind eye' to fake or substandard goods. Here the major driver is price, where the temptation to purchase is ever higher according to the perceived quality of the imitation, correlated with the size of the price differential between imitation and genuine article. Even when the goods are genuine, there are price incentives for both suppliers and consumers to avoid knowing that products result from bad practices such as child labour, environmental abuses, or supporting war zones and other human rights malpractices. Increasingly, however, many consumers are interested in the authenticity and provenance of their goods and services, would like to avoid bad production practices, and be assured that the origins of their foods, cosmetics and other products are as claimed.

Markets for high-value products are increasingly making claims to particular origins and methods of production and quality. Almost all of these are attractive as potential markets for fraudulent imitations or cheap 'rip-offs'. They encompass food, drink, perfumes and cosmetics, jewellery and other accessories, electronics, clothes and many other products. In every case, modern technology could do more to assure the supply chain and provenance of the products.

Vladimir Šucha and colleagues from the Joint Research Centre set out key issues for the food and drink sector in Chapter 11. Traceability is crucial and can involve overt technology such as holograms and colour-shifting ink, or covert technology such as tags based on DNA printing inks. Synthetic and unique DNA can be incorporated in packaging and is impossible to forge.

In Chapters 10 and 11, the authors discuss the potentially rich sources of information about the provenance of goods. Careful measurements can exploit subtle geographic differences in naturally-occurring isotope ratios to test claims about product origin: which ocean did this fish come from? Was this chemical made in factory X or factory Y? Were these grapes grown in region A or region B?

There are other domains where forensic analysis can provide important evidence on the source of goods. For example the important use of nuclear forensic analysis to determine the origin of radionuclides is explored in two case studies on p112 and p116 of Chapter 10.

Analytical sciences already play a major role in assuring pharmaceutical markets. The first

challenge is to ensure the quality of the product. The second is how to detect counterfeit medicines and other medical products and devices that are intended to deceive, and eliminate these from the supply chain. Innovative use of existing technologies has allowed the pharmaceutical industry to use anti-counterfeit technologies. In Chapter 12, Harparkash Kaur discusses how drugs can be tracked and traced using a variety of techniques from radio identification to 'NanoEncryption'. A third challenge in pharmaceutical markets is the global regulation of intellectual property, different in type from the first two (yet sometimes conflated unhelpfully with them). The challenge here is to balance the interests of the inventor with the interests of different market places to achieve affordable supplies of goods and services that are seen around the world as 'public goods'. This goes well beyond the scope of the analysis in this report.

Looking more broadly, forensic approaches to DNA and RNA sequence analysis can track the origin and spread of bacterial and viral diseases and combine this analysis with genetic markers of antibiotic sensitivity or resistance. And in her case study on p94, Lucy Webster explains how DNA analysis helps in combatting the illegal trade in wildlife, for instance by ensuring that an original (legal) trophy is not illegally re-sold and replaced with a fake.

Technology for authentication requires the characterisation of a unique marker of the product or its component parts. This marker can be intrinsic to the product or a signature marker that is added as part of the production process. In the case of biological products, these come with their own DNA signatures. Similarly, many other physical and chemical products bring with them their own natural molecular or atomic signatures. Alternatively, unique identifiers that can be biological, chemical, physical or digital can be added to products that can be traced throughout the supply chain. For example, for printed objects it is possible to go well beyond existing printed codes on the banknote, the driving licence or passport. Microscopic analysis of the surface on which the code is printed has the potential to provide a two - or even three-dimensional unique signature that can be correlated with the printed code, providing robust two-step assurance of the identity of the object.

It is one thing to be able to add a signature; it is another to detect it accurately, reliably and cheaply. This is where technology is advancing. An expanding market place for even better equipment could drive rapid advances in technology.

The fourth key message that is of increasing importance and urgency is how we assure the identity of people on the internet, whether they are consumers or providers of goods and services. Even if this is not possible or desirable, we need to be able to authenticate the claims of people in cyberspace to represent an organisation, be a reliable purchaser or supplier of goods and much else besides. Sue Black explores the need for proof of identity further in Chapter 6.

Cyberspace provides a rapidly growing marketplace where it is easy to conceal, create and steal identities for both individuals and organisations. Any active internet user requires multiple passwords, and it is not easy for us frail humans to carry out best practice in password protection and usage. This is an area where we need technology to provide solutions for the problems created by our invention and use of technology in the first place. Technological solutions here include password creation and management tools, two-step authentication processes, coupled digital and biometric tools and secured connection protocols.

A significant new deployment of digital techniques, mentioned earlier, is the development of distributed ledgers. This technology is already being applied to high-value goods such as diamonds to assure their provenance, history of ownership, and to exclude 'blood diamonds' from the marketplace.

Meanwhile, environmental applications and the opportunities for ensuring adherence to regulation are brought out by Ian Boyd in Chapter 14, which provides some excellent examples to others in government as to how

these techniques might be used. The case of the great crested newt illustrates how, using DNA detection techniques, a commercial tool was developed to quickly and cheaply detect the presence of these creatures. Within the planning process it is estimated that businesses are likely to have saved over £2 million in survey costs in 2015 alone thanks to the introduction of this environmental DNA test.

It is obvious that there is huge potential for technology to provide consumers with genuine goods of assured provenance. Technology can also help us to know the true identity of individuals or organisations with whom we interact in cyberspace. **The fifth key message** of this report is that the UK has the opportunity to be a world leader in the development and use of technology for prevention, deterrence and detection of fraudulent products and services. This in turn will provide significant opportunities to promote our own products and services.

However, many of these solutions bring added costs and neither producers nor consumers have the strongest incentives to apply them for anything other than very high-value goods.

The questions to policymakers are:

- What are the products and services where it is most important to assure supply chains and authenticity?
- Do standards, regulation, accreditation and enforcement mechanisms need to be strengthened to drive markets that will implement existing and new technologies to assure the identity and provenance of goods and services?
- What further steps should be taken to encourage the implementation of online technologies and behaviours to assure the identity of both consumers and providers of online products and services?
- What is the role of standards, accreditation and kite marks to help both consumers and providers of goods and services?

CAPTURING THE OPPORTUNITIES FOR THE UK

As forensic approaches continue to spread well beyond the courtroom, the UK needs to retain strong drivers for innovation and to enable the innovative effects of the new technologies themselves to be applied across a very wide range of public and private sectors.

New forensic techniques offer the prospect of more robust and efficient forms of regulation in areas from nuclear safety to food security. Therefore they must be subject to robust standards and accreditation, based on agreed levels of rigour and repeatability.

Government inevitably has an important role, creating the framework of regulation, skills and investment that will enable researchers and businesses to stay at the forefront of international markets, and to enable them to take best advantage of the fact that the UK is the only country in the world where the delivery of forensic science has been commercialised. However, with a relatively small direct market for forensic techniques, and generally transactional relationships between supplier and customer, there is little long-term certainty in provision.

Potential innovators need the mix of collaboration and competition that will best enable investment in innovation. In Chapter 16, Geraint Morgan, Thomas Bassindale and Mark Pearse set out the case for a sector specific approach. In Chapter 17, Mark Littlewood and Gillian Tully describe how the UK might exploit its current high standing in the traditional forensic disciplines to capture more of the expanding international markets for forensic services.

Innovations in other sectors, such as defence or medicine, are likely to be important for the development of forensic science capabilities and vice versa. Therefore, **the sixth key message** is that innovators should be encouraged to go well beyond the traditional boundaries of forensic science and to think more broadly about potential applications in new markets and new forms of public service delivery. As well as the development of novel uses of existing techniques, future developments in areas such as genomic science, data sciences including information technology and machine learning, the Internet of Things, and quantum technologies – and the interactions between

them – will create new opportunities. Chapter 17 of this report provides insights into accessing the market and describes the processes involved.

Our last two questions for policymakers are:

Q How should we best measure and assure the impact of innovation in forensics on the wider landscape: in both the provision of forensic services internationally, and in enabling trustworthy markets in the full range of business sectors?

Q How can government catalyse and shape the marketplace to allow for greater innovation, exploitation, adoption and long-term investment in forensic approaches themselves, including drawing on all potentially relevant disciplines?

THE FUTURE OF FORENSIC SCIENCE

Forensic science draws on almost every discipline. This broad landscape comes with its own challenges and opportunities in attracting funds to the right places and ensuring the best return on investments in people, tools and techniques. Its applications, as illustrated here, extend across the Criminal Justice System and beyond. Relevant innovation can come from almost anywhere, and be applied in seemingly wholly unrelated fields. For instance, distributed ledger technology developed for the purposes of a cryptocurrency is already being applied to other disparate areas where there is need to assure provenance and assurance of ownership. Therefore the research, innovation, policy, law enforcement and commercial communities need to find better ways of ensuring the cohesion and connectedness that will enable the UK to get the biggest possible benefit from these trends.

Forensic techniques can be used to demonstrate provenance and authenticity in ways that could increase confidence in markets and, in some cases, create new business models. Knowing, with a high degree of assurance, the provenance of food or clothes, or the authenticity of the antique or the exotic, will offer opportunities for businesses to add value in new ways.

This report seeks in part to challenge the boundaries of various sectors, to look creatively at what others are doing and encourage innovation across sectors. This will lead to a rich ecosystem of forensic and analytical science, while contributing to our nation's prosperity by ensuring the authenticity, provenance and assurance of our physical and virtual world, both inside and outside of the courtroom.

In conclusion, there are important existing and new opportunities for the application of forensic and analytical science and technology. The need for the effective application of these is growing rapidly as citizens increasingly use and provide globalised markets and services, and, in doing so, expand the uses of the internet and world wide web. The purpose of this report is to stimulate the imagination of those inside and outside the existing world of forensic and analytical sciences to think how to improve and develop new applications of forensics. The purpose is also to challenge policymakers with some key questions. The policies developed in response to these questions could enable the realisation of more benefits from existing and emerging forensic approaches whilst minimising the risks of their inappropriate application or mis-application. Forensic and analytical science and technology are needed for our resilience, security and prosperity by assuring the authenticity and provenance of goods, people and organisations, both inside and outside of the courtroom.

This publication is available from www.gov.uk/go-science

Contact us if you have any enquiries about this publication, including requests for alternative formats, at:

Government Office for Science
1 Victoria Street
London SW1H 0ET
Tel: 020 7215 5000
Email: contact@go-science.gsi.gov.uk

GS/15/37A