Proof is Not Binary: The Pace and Complexity of Computer Systems and the Challenges Digital Evidence Poses to the Legal System

JOHN S ATKINSON[*]

This article illustrates the challenges that an 'information society' poses to the current and future legal system and how the complexities of digital evidence itself have helped pave the path to the current privacy and surveillance status quo. We now live in a society where interaction with computer technology is unavoidable. At the heart of the privacy and surveillance debate lies the ability (or inability) to collect data from digital devices. Any of this data is potentially digital evidence, either in a strict legal sense or merely because it reveals something that would otherwise remain private.

Previously collection of digital evidence at today's scale would be utterly impractical. Furthermore, while the evidence itself could be as mundane as a photograph, the multiple computer systems that supply it will be highly dynamic, difficult to explain, and capable of automated decision-making. The legal system is left constantly trying to catch up with a relentless technological pace, with precedent set in wholly different contexts, and reliant on a digital forensics field still in its infancy. The logical aspect of digital evidence stretches traditional concepts of custody and jurisdiction. Simultaneously, the complexity and pace of modern technology necessitates a departure from prior (non-digital) forensic culture.

[*] PhD candidate in Security and Crime Science, University College London (email: j.atkinson@ee.ucl.ac.uk).

1. Introduction

This article illustrates the challenges that an 'information society' poses to the current and future legal system and how the complexities of digital evidence itself have helped pave the path to the current privacy and surveillance status quo in the UK. It is intended for a mostly non-legal, non-technical audience and although primarily concerned with the law of England and Wales, calls upon academic literature and comparable legal precedent worldwide.

We now live in a society where interaction with computer technology is increasingly unavoidable and this trend is only set to continue. At the heart of the privacy and surveillance debate lies the ability (or inability) to collect data from digital devices, control its existence or availability, and determine its accuracy. Any of this data has the potential to be digital evidence, either in a strict legal sense or merely because it implies something that would otherwise have remained private.

Even twenty years ago, collection of digital evidence on the scale possible today would have been utterly impractical. Furthermore, while the evidence itself could be as apparently mundane as a photograph, the multiple computer systems that now supply it are likely to be highly dynamic, difficult to fully explain to a non-expert, and capable of (at least) basic automated decision-making.

The legal system is left constantly trying to catch up with a relentless technological pace, with precedent set in wholly different contexts, and reliant on a digital forensics field still in its infancy. The logical aspect of digital evidence challenges existing legal procedure as it stretches traditional concepts of custody and jurisdiction. Simultaneously, the complexity and pace of modern computer software necessitates a departure from the prior (non-digital) forensic culture.

2. What exactly is Digital Evidence?

Digital evidence may be gathered from a great variety of electronic systems. While the evidence itself can be something apparently mundane, such as a digital photograph, the computer system supplying it is likely to be highly complex, dynamic and difficult to fully explain to a non-expert. We now live in a society where computer technology is increasingly commonplace. However, academic study within the field of court-admissible 'digital forensics' only began as recently as 1992.[1] As the use of digital evidence is now essential, tools and forensic techniques used for its collection and analysis must be created and modified as often as the systems themselves. Unlike other forensic disciplines, collecting and archiving potential evidence from digital systems is easily automated.

2.1 Definitions

The Scientific Working Group on Digital Evidence defines digital evidence as follows:

> ***Digital Evidence:*** 'Information of probative value that is stored or transmitted in binary form'.[2]

As a practitioner in this field, Barbara elaborates upon how forensic discipline relates to this:

> ***Digital Forensics:*** 'The application of science and technology to the identification, recovery, transportation, and storage of digital evidence ... Digital forensics is a relatively new forensic science'.[3]

These definitions are incredibly broad and far from limited to only traditional desktop computers and local area networks in offices. Less obvious examples range from mobile phones and passports to traffic lights and washing machines. The very idea that an appliance or inanimate object is potentially capable of tracking a person's activities—let alone support or disprove a statement in court—is shocking.

[1] Eugene H Spafford, 'Some Challenges in Digital Forensics' in Martin S Olivier and Sujeet Shenoi (eds), *Advances in Digital Forensics II* (Springer 2006).

[2] Scientific Working Group on Digital Evidence (SWGDE), 'Digital & Multimedia Evidence Glossary' (v2.7, *SWGDE*, 8 April 2013) 7 <www.swgde.org/documents/Current%20Documents/2013-04-08%20SWGDE-SWGIT%20Glossary%20v2.7> accessed 18 November 2014.

[3] John J Barbara, *Handbook of Digital and Multimedia Forensic Evidence* (2nd edn, Humana Press 2008) 11.

Furthermore, Kipper notes the pace of technological change and aptly likens it to the growth of a child, where the combined effect of many subtle changes may not be obvious to those who observe them daily. He notes that experts may 'not always recognize or understand the change until a significant time period has elapsed or until others have pointed it out'.[4] Digital forensic practitioners may be required to justify and explain evidence in court, which is difficult as computer systems are built from *layers* of technology. An expert in one field is unlikely to, and possibly incapable of, fully understanding the ever-changing nuances of the contiguous technological layers their expertise rests upon. Similarly, developers and operators of technology are unlikely to fully comprehend the potential use (or misuse) of the data they hold without specifically looking to analyse them.

This article is concerned with two categories of digital evidence. First, the evidence used in a court of law, which should meet admissibility criteria. Second, evidence for suspecting an individual of committing a crime. This may be the evidence required to obtain a warrant or justify 'reasonable suspicion' leading to questioning, search or arrest.

2.2 Using and 'Handling' Digital Evidence

The UK Association of Chief Police Officers provides 'good practice' guidelines on how digital evidence for use in court should be handled. A summarized version follows:

- The original data must not be changed.
- Any person accessing the original data must be competent and able to explain the relevance and the implications of their actions.
- All processes applied to an exhibit should be recorded and must be repeatable by an independent third party.

[4] Gregory Kipper, *Wireless Crime and Forensic Investigation* (Auerbach Publications 2007) xvii.

- The person in charge of the investigation has responsibility for ensuring that the law and these principles are adhered to.[5]

These guidelines differ little from other forensic disciplines and, notably, are not a legal requirement. There are more thorough guidelines for expert practitioners, such as those produced by Mason[6] or Kipper,[7] but ultimately the validity of evidence is determined by the court following expert witness testimony. Neiditz, Safer and Hatfield note that digital evidence is often accepted with little scrutiny.[8] He highlights the uncommon ruling in *Lorraine v Markel* (US) where email evidence was found to be inadmissible.[9] Exhibited printouts, although routinely accepted as evidence and clearly 'real', were discounted because no attempt had been made to validate their authenticity.

Practitioner guidelines make the distinction between securing the logical and physical aspects of digital evidence. While practices for securing physical evidence have been refined over hundreds of years, logically securing data is an ill-defined and complicated process as will be discussed further in Section 3.2. Distributed technology like the internet can even complicate physically securing evidence because original copies of data may be physically inaccessible or held outside of legal jurisdiction. Lloyd notes that 'there is a need for a massive effort to secure international consensus and harmonisation'.[10]

[5] Association of Chief Police Officers, *Good Practice Guide for Computer-Based Electronic Evidence* (v4.0, *7Safe*, 2011) <www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence_v4_web.pdf> accessed 21 November 2014.

[6] Stephen Mason (ed), *Electronic Evidence: Disclosure, Discovery and Admissibility* (3rd edn, Butterworths Law 2012).

[7] Kipper (n 4).

[8] Jon Neiditz, Jay Safer and Pat Hatfield, 'United States: From E-Discovery to E-Admissibility? "Lorraine v. Markel" and What May Follow' (*Mondaq*, 8 June 2007) <www.mondaq.com/unitedstates/article.asp?articleid=49160> accessed 3 August 2014.

[9] *Lorraine v Markel* 241 FRD 534 (2007).

[10] Ian Lloyd, *Legal Aspects of the Information Society* (Butterworths Law 2000) 127.

3. Parting with Tradition

3.1 The Good: Efficient Automation and Electronic Records

A major driving force behind the growth of computer technology is the promise of rapid and cost-efficient access to information with reduced administrative overheads. In terms of digital evidence for law enforcement, *TotalRoam* and its successor systems embody this.[11] Through the installation of computers in police patrol cars, the system instantly provides information on vehicle registration and outstanding warrants to guide the efforts of law enforcement. Furthermore, data such as patrol location and breathalyser results can be automatically recorded and immediately archived without paperwork. It is easy to see how these systems are convenient. However as we will shortly discuss, given the complexity of the systems involved, ensuring this information retains its integrity (stays the same), authenticity (can be proven to be from a trusted source) and confidentiality (only seen by those who should see it) is likely to be far more difficult digitally than it might have been with familiar physical methods.

New technology also allows for evidence to be collected on an unprecedented scale as has been shown by the modern practice of electronically tagging lesser offenders. Evidence can be collected automatically to determine whether parole conditions are violated and can provide immediate notification when this is the case. In addition, knowledge of this acts as a deterrent. Kipper states the scheme is 95% successful,[12] however the legitimacy of such figures has been disputed.[13] Similarly, the London congestion charge implements public regulations that would have previously been impractical.[14] Schemes like the congestion charge are several steps

[11] Kipper (n 4).

[12] ibid 46.

[13] Mike Nellis, 'The Electronic Monitoring of Offenders in England and Wales: Recent Developments and Future Prospects' (1991) 31(2) The British Journal of Criminology 165.

[14] Transport for London, *What Do I Need to Know about the Congestion Charge Camera System?* (*TfL*, 2011) <www.tfl.gov.uk/assets/downloads/CC-Cameras.pdf> accessed 3 August 2014.

further along than mere efficient electronic records because they also feature almost entirely automated enforcement.

3.2 The Bad: Intangible Data

The guidance for expert practitioners makes a clear distinction between the logical and physical aspects of digital evidence. While there are hundreds of years of precedent for securing physical evidence, digital evidence provides a unique challenge in that it must be kept logically secure as well.

Rules of best practice for traditional forensic evidence are established through knowledge of consistent physical laws and observation. In contrast, laws governing digital systems can often be rewritten and modified at will. Even when physically seizing evidence is possible, how should a 'first responder' best preserve evidence on a computer found switched on? Should it be left running when it might be purging data? Should it be turned off normally and potentially trigger a 'clean-up' process? Should the power cord be pulled and risk data corruption? Best practices can only ever be effective in the general case. However, the general case for digital evidence can be significantly narrower than those for other types of forensic evidence because the rules of the systems involved can be modified.

It may not be obvious until pointed out, but deliberately hiding information is actually a fundamental concept of hardware and software engineering: a user interface provides a reduced set of functionality, software abstraction allows programmers to use code without knowing the implementation, and your web browser does not care whether the page on display arrived via LAN cable, WiFi, SD card, or carrier pigeon. If this were not the case then using and developing modern technologies would be effectively impossible. This is a double-edged sword for the legal system. While this may provide a wealth of digital evidence to forensic investigators, it raises questions of how far one should go to validate any given detail.

For the logical aspect of digital evidence, the idea of 'handling' it is a complete misnomer. Data is just a representation and never moved; it is copied. It is often assumed that the first copy is deleted but this may not occur until it is convenient for the system, or not at all.

Recovering discarded and hidden information is a major part of the digital forensics field. This can be a huge boon for law enforcement because evidence of unlawful activity is potentially more plentiful and difficult to destroy or conceal without preparation.

However, with some preparation and foresight digital evidence can also be deliberately hidden very easily. Strong encryption, for example, can be used and in many cases cannot be broken practicably by law enforcement. Cryptography is incredibly complex, but you don't need to be an expert to follow an internet tutorial on using a free program. This problem has led to legislation that makes failure to divulge a cryptographic key or password to law enforcement punishable as a criminal offence under UK law, with penalties up to two years in jail.[15]

This is arguably at odds with the 'right to remain silent' and effectively shifts the burden of proof from the prosecution to the defendant. It also implicitly affords the state the right to access any encrypted data and has drawn criticism from security experts such as Anderson[16] and Schneier[17] who view it as an ill-conceived response to a technology that appears threatening. In addition, they question the effectiveness of such laws given that serious crimes are likely to attract sentences longer than two years.

3.3 The Ugly: Unverifiable Software

This is further complicated because the tools used to analyse digital evidence are software themselves. In fact, the general undecidability of program behaviour (the 'Halting Problem') is a fundamental tenet of computer science.[18] Formal proofs of software are slow, expensive,

[15] Regulation of Investigatory Powers Act (RIPA) 2000.

[16] Ross Anderson, 'RIPA III: A Legislative Turkey Comes Home to Roost' (*The Register*, 25 November 2009) <www.theregister.co.uk/2009/11/25/jfl_ripa_opinion/> accessed 3 August 2014.

[17] Bruce Schneier, 'UK Police Can Now Demand Encryption Keys' (2007) *Schneier on Security* <www.schneier.com/blog/archives/2007/10/uk_police_can_n.html> accessed 3 August 2014.

[18] Alan Turing, 'On Computable Numbers, with an Application to the Entscheidungsproblem' (1936) 42(2) Proceedings of the London Mathematical Society.

difficult and rarely seen outside of small components in safety-critical engineering. Even then, they only show that software fulfils a given model, not that the model itself is correct, nor that a program correctly implements it. Fundamentally, both programs and data are just a sequence of binary digits. These will undergo an arbitrary number of transformations, re-interpretations, error corrections and retransmissions before being presented to the user. At what point should a mess of ones and zeroes be trusted either as evidence, or to provide it?[19]

There has been some work towards digital equivalents of physical forensic procedures. For example, Richard and Roussev propose a system of 'digital evidence bags' which encapsulate essential data to provide forensic integrity and audit trails.[20] They stress the 'urgent need for a digital-forensics-aware operating system'. While this adds yet more complexity, this is probably the only practicable solution.

4. Centralised for Complexity

4.1 Industrial Expertise

Previously, the UK FSS (Forensic Science Service) was tasked with overseeing digital forensic procedure in UK criminal cases but closed on grounds that it was not cost effective. Forensic work was outsourced to either police laboratories or private companies with no central authority.[21] But even before this decision, the complexity of forensic software has led to the domination of the industry by a select hegemony of international companies. For example, *EnCase* software has become the '*de facto* standard' in criminal investigations and the majority of digital forensic work is performed

[19] Sergey Bratus, Ashlyn Lembree and Anna Shubina, 'Software on the Witness Stand: What Should It Take for Us to Trust It?' [2010] Trust and Trustworthy Computing: Third International Conference 396.

[20] Golden G Richard III and Vassil Roussev, 'File System Support for Digital Evidence Bags' in Martin S Olivier and Sujeet Shenoi (eds), *Advances in Digital Forensics II* (Springer 2006).

[21] Nina Lakhani 'CSI Chief Condemns Forensic Cuts' *The Independent* (London, 9 January 2011).

by large consultancies, such as KPMG or PwC, whose traditional competencies are in business intelligence and financial auditing.[22]

Even before the closure of the FSS, there existed a large disparity in cultures surrounding different forensic disciplines. While DNA and fibre analysis have deep roots in academic science, software companies and programmers are primarily concerned with engineering. The difference between scientific and software engineering cultures may be vast.[23] The typical software business model is the very antithesis of open peer review; source code[24] is a trade secret, patents are commonplace and reverse engineering mostly unlawful.[25]

This lack of transparency has proven problematic in recent drink-driving prosecutions in the USA where the court's attempt to make breathalyser source code available was opposed by the manufacturer. Despite having been used as the sole evidence leading to prior convictions, eventual examination concluded that the code was 'below industry-standard best practices' and contained errors.[26] There is a danger that the field of digital forensics is growing as a business venture in search of profit, rather than scientific validity.

4.2 A Forensics Arms Race

As well as tools for general security (e.g. encryption), the dominance of certain forensic software has also led to a situation where 'anti-forensics' software is specifically designed to thwart the abilities of

[22] Simson L Garfinkel and others, 'Advanced Forensic Format: An Open Extensible Format for Disk Imaging' in Martin S Olivier and Sujeet Shenoi (eds), *Advances in Digital Forensics II* (Springer 2006).

[23] Henry Petroski, 'Reference Guide on Engineering Practice and Methods' in *Reference Manual on Scientific Evidence* (2nd edn, Federal Judicial Center, Washington DC 2000).

[24] Source code: a computer program as written by a programmer.

[25] Council Directive (EC) 2009/24 of 23 April 2009 on the legal protection of computer programs [2009] OJ L111/16.

[26] Ryan Paul, 'Buggy Breathalyzer Code Reflects Importance of Source Review' (*Ars Technica*, 15 May 2009) <arstechnica.com/tech-policy/2009/05/buggy-breathalyzer-code-reflects-importance-of-source-review> accessed 3 August 2014.

common tools.[27] One person's security is another's obstruction and, as seen with illegal filesharing, there is no way to easily control the proliferation of software. The public, businesses, law enforcement, and criminals all have similar security measures and forensic tools available. The state is therefore placed in an odd position where it must ensure that systems are both resilient (to prevent crime) and vulnerable (for the state's own investigative purposes) simultaneously.

This issue was epitomised by the FBI's 'magic lantern' software. Although used to gather evidence, it was functionally indistinguishable from viruses or criminal keylogging software used to steal credit card information and passwords. To be of any lasting use, the scheme would have required the complicity of anti-virus vendors and was met with guarded disdain. Without the ability to guarantee the software operator was legitimate, this would have effectively given free access to any intruder.[28]

More recently, leaked documents have implicated the US National Security Agency (NSA), GCHQ, and other partners, in the deliberate sabotage of international encryption standards and installation of secret 'backdoors' into the networks of large internet companies. Security practitioners expressed outrage at such conduct, noting that this traded the long-term security of users worldwide (including those within the US and UK) for the short-term advantage of a certain few agencies. Again, once discovered, such weaknesses could be used by anyone.[29]

[27] Simson L Garfinkel, 'Anti-Forensics: Techniques, Detection, and Countermeasures' (2nd International Conference on i-Warfare and Security, California, 8-9 March 2007) 77 <http://simson.net/clips/academic/2007.ICIW.AntiForensics.pdf> accessed 21 November 2014.

[28] Neal Hartzog, 'The "Magic Lantern" Revealed: A Report of the FBI's New "Key Logging" Trojan and Analysis of its Possible Treatment in a Dynamic Legal Landscape' (2002) 20(2) John Marshall Journal of Computer and Information Law 287.

[29] Nicole Perlroth, Jeff Larson and Scott Shane, 'N.S.A. Able to Foil Basic Safeguards of Privacy on Web' *New York Times* (New York, 5 September 2013) <www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?pagewanted=all> accessed 3 August 2014.

4.3 Deliberate Abuse

The case of *R v Weiner* is both a triumph for digital forensics and cause for concern.[30] Weiner planted 'evidence' of child pornography on the computer of his colleague, Eddie Thompson. Although the deception was eventually uncovered when the original 'anonymous' phone call warning police was traced back to Weiner, the judge noted that 'his plot to have Mr Thompson sacked and prosecuted very nearly succeeded'.[31]

Perhaps even more worrying are the actions of ACS:Law and similar firms. Ostensibly legitimate legal and forensic specialists like those in Section 4.1, they sent thousands of letters demanding hundreds of pounds in settlements from alleged copyright infringers. They then attempted to drop the few cases that did reach court after their legal merit was heavily criticised. This was denied after the presiding judge called it an attempt to 'avoid judicial scrutiny' of the underlying claims and denounced their 'wholesale letter writing campaign' which was likened to blackmail by the defence because of the large costs required to defend such a case.[32] This is in great contrast to the traditional role of impartial forensic experts in court and is currently under close scrutiny. While similar circumstances of joint collection and demand for settlement exist, they are far less severe. Parking tickets operate on similar principles but involve much less money and an appeal process where the accused can defend themselves much more easily. Similarly, insurance companies can employ their own forensic fire investigators when arson is suspected but (in stark contrast to ACS:Law's methods) Clarke notes that prosecution is 'a recourse reserved for the most flagrant instances, because it demands a high standard of proof'.[33]

[30] *R v Weiner* [2011] EWCA Crim 1249, [2012] 1 Cr App Rep (S) 24.

[31] 'Handyman Jailed for Planting Porn on Boss's Computer' (*BBC News,* 23 September 2010) <www.bbc.co.uk/news/uk-england-london-11397515> accessed 3 August 2014.

[32] Gary Moss, '*Media CAT v Adams*: The CAT that Did Not Get the Cream' (2011) 6(11) Journal of Intellectual Property Law and Practice 6.

[33] Michael Clarke, 'The Control Of Insurance Fraud: A Comparative View' (1990) 30(1) British Journal of Criminology 1.

5. Implications of an 'Information Society'

5.1 Continual Monitoring

As has been seen with the electronic tagging of offenders and automatic traffic systems (Section 3.1), technology now allows individuals to be put under continuous observation. This can be done on a large scale and potentially without the target being aware. The legality of this is inconsistent. For example, public CCTV requires the operator have signs to inform those under observation.[34] In contrast, internet service providers are required to record details of email correspondence and other web activity without users being explicitly informed.[35]

The ability to monitor activities covertly and easily is an attractive idea to the security services. Examples include warrantless wiretapping by the NSA and AT&T in the USA[36] as well as controversial proposals by police in the UK to track vehicle movements for up to two years.[37] While these may indeed be useful, civil liberties organizations are concerned that there is little oversight of such programmes. This is especially true in the case of warrantless wiretapping where litigation was prevented because it 'would require the government to disclose privileged "state secrets"'.[38] Civil liberties groups contend that such systems bypass usual privacy protections by removing the burden of evidence required to place a suspect under surveillance.

Programmes that allow observation without affording the observed the ability to know whether this is truly the case are likened to the concept of 'panopticon'. This was originally proposed by Bentham as a proposed prison design which provided a 'sentiment of an invisible omniscience' and 'a new mode of obtaining power of mind

[34] Data Protection Act 1998.

[35] Anti-Terrorism, Crime and Security Act 2001.

[36] Electronic Frontier Foundation, 'Our Work: NSA Spying' (*Electronic Frontier Foundation*) <www.eff.org/issues/nsa-spying> accessed 3 August 2014.

[37] Emma Smith and Dipesh Gadher, 'Spy Cameras to Spot Drivers' Every Move' *The Sunday Times* (London 13 November 2010).

[38] Electronic Frontier Foundation, 'Jewel v. NSA' (*Electronic Frontier Foundation*) <https://www.eff.org/cases/jewel> accessed 3 August 2014.

over mind' that was hoped would enforce good inmate behaviour with minimal personnel.[39] Brignall writes that as these technologies become a cultural necessity, they provide worryingly broad opportunities for social control.[40]

5.2 Data Mining and Retroactive Enforcement

Cardinal-Duc de Richelieu famously wrote, 'Give me six lines written by the hand of the most honest of men, I will find something in them which will hang him'.[41] It is interesting to consider the potential implications of indefinitely archiving the everyday actions of individuals. There is no time limit for prosecution to be brought for most offences in the UK, nor is ignorance of the law a valid defence.[42] While it is incredibly easy to collect data, processing it is more difficult. Deciding what might be useful evidence is even harder and, ultimately, the number of prosecutions that can be brought to court is limited. The quantities of data capable of being retained can be problematic even on common consumer systems, let alone the large surveillance programmes discussed. As datasets grow increasingly larger, heuristic techniques for 'data mining' have been developed.[43]

The disparity between available data versus the ability to process, investigate and prosecute necessitates some form of selection process. This would be retroactively discovering crimes and is notably distinct from the current practice of collecting forensic evidence (e.g. DNA) for later conviction (or appeal) when it has already been established that a crime may have occurred. Furthermore, potential evidence of wrong-doing need not be held and managed by the state.

[39] Jeremy Bentham, 'Panopticon; Or the Inspection-House' (1787) in Miran Bozovic (ed), *The Panopticon Writings* (Verso 1995) 29.

[40] Tom Brignall III, 'The New Panopticon: The Internet Viewed as a Structure of Social Control' (2002) (3)1 Theory and Science 1527.

[41] Cardinal-Duc de Richelieu, First Chief Minister of France (1624–1642).

[42] Edwin R Keedy, 'Ignorance and Mistake in the Criminal Law' (1908) 22(2) Harvard Law Review 75.

[43] Mark Pollit and Anthony Whitledge, 'Exploring Big Haystacks' in Martin S Olivier and Sujeet Shenoi (eds), *Advances in Digital Forensics II* (Springer 2006) 67.

Instead historic data may be held as a matter of course by private companies as part of their service. Given past instances of 'gaming strategies' to hit performance targets, there is potential that the convenience of technology will shift focus onto crimes which are now the simplest to prosecute, rather than those in the community interest.[44]

Resistance against this has been reflected in recent legislation by the European Union that recognises the 'right to be forgotten'. It proposes that citizens 'shall have the right—and not only the "possibility"—to withdraw their consent to data processing'.[45] However, writers familiar with the workings of the internet wonder whether this proposal is actually possible to practically implement or enforce.[46] Attempts to apply the right to be forgotten have been met with ire from organizations that consider themselves to produce factual publications. National newspapers, broadcasters and referenced works like Wikipedia complain that these laws are being used only by the privileged to improve their image by 'censoring' negative search engine results.[47]

5.3 Automated Justice?

Software for digital forensics began with retrieving data, then aiding interpretation. Now software 'can be used by investigators to determine which evidence can be trusted'.[48] While this progression is logical, care should be taken to consider whether it is acceptable to defer these decisions to programs or software companies. Given the

[44] Barry Loveday, 'Policing performance: The Impact of Performance Measures and Targets on Police Forces in England and Wales' (2006) 8(4) International Journal of Police Science and Management 282.

[45] Jacob Aron, 'A Right to be Forgotten Online? Forget it' *New Scientist* (London, March 2011).

[46] Jeffrey Rosen, 'The Web Means the End of Forgetting' *New York Times* (New York, 21 July 2010).

[47] Alex Hern, 'Wikipedia Swears to Fight "Censorship" of "Right to be Forgotten" Ruling' *The Guardian* (London, 6 August 2014).

[48] Marika Wojcik and others, 'Applying Machine Trust Models to Forensic Investigations' in Martin S Olivier and Sujeet Shenoi (eds), *Advances in Digital Forensics II* (Springer 2006) 55.

lack of competitive diversity between these companies, as discussed in Section 4.1, any error threatens a potentially disproportionate impact on a large number of cases. Despite software mistakes or 'bugs' being estimated to cost $100 billion in the USA alone, software companies are not usually held liable.[49] This is in great contrast to the responsibilities of expert witnesses providing forensic evidence, who will be professionally discredited or potentially struck off when mistakes are made.

Looking ahead, modern systems like IBM's 'Watson' have been shown to be capable of interpreting natural language, reasoning and answering complex questions. Although currently famed for 'merely' defeating the human all-time champions of the US quiz show *Jeopardy!* unaided, there is now serious industrial and academic effort being applied to use the technology behind 'Watson' as a legal authority.[50]

Perhaps unexpectedly, there is already some legal precedent for this kind of trust in automated decisions. The Data Protection Act (1998) explicitly requires individuals to be notified when autonomous decisions are taken (e.g. for a loan application) and grants them the right for it to be reconsidered manually.[51] However, exemptions apply to decisions if they are required by other legislation and many of the principles outlined in the act do not apply to 'national security', criminal investigations or taxation efforts. The recent case of Mohammed Kabay[52] who falsely accused Samsung of installing key-logging software on its laptops shows the danger in

[49] Dominic Callaghan and Carol O'Sullivan, 'Who Should Bear the Cost of Software Bugs?' (2005) 21(1) Computer Law and Security 56.

[50] Robert C Weber, 'Why "Watson" Matters to Lawyers' (*The National Law Journal*, 14 February 2011) <www.nationallawjournal.com/id=1202481662966/Why-Watson-matters-to-lawyers?slreturn=20141021162613> accessed 21 November 2014.

[51] Data Protection Act 1998.

[52] Associate Professor of Information Assurance at Norwich University and Chief Technical Officer of Adaptive Cyber Security Instruments Inc.

unquestioningly trusting the judgements of computer tools and how easily it is done, even for experts.[53]

6. Conclusion

The logical aspect of digital evidence challenges existing legal procedure as it stretches traditional concepts of custody and jurisdiction. Digital forensics is a field still in its adolescence, so instances of misuse are perhaps inevitable given the lack of experience. The potential for abuse should be mitigated with time and precedent. The appropriateness of demanding encryption keys should also be resolved as the technology becomes banal and investigators encounter it regularly.

While it appears that industrial consolidation is economically inevitable given the quantity and complexity of technological systems, common software engineering practice is unsuitable to retain the integrity of forensic discipline. Much greater openness is required than is generally found in business culture. The inner workings of tools and procedures should be transparent. This will support more thorough validation, and anti-forensics tools will continue to exist regardless. Although guarantees of correctness are impossible, this would afford digital evidence much greater credibility, despite complexity preventing full explanations in court.

Intelligent systems allow for increasingly automated collection and analysis of evidence. These can be incredibly useful tools, but care should be taken to ensure that the crimes easily monitored and discovered by these systems (the 'low hanging fruit') do not take priority as an unintentional side-effect of their adoption. Despite the temptation to trust such systems, transparency is vital to understand the processes behind their results so they can be critically examined with context.

[53] Mohammed E Kabay, 'Apology to Samsung: We Blew It' (*Network World*, 4 April 2011) <www.networkworld.com/ newsletters/sec/2011/040411-sec-apology.html> accessed 3 August 2014.