International Journal of Cyber Criminology
Vol 9 Issue 1 January – June 2015

ISSN: 0973-5089 - January – June 2015. Vol. 9 (1): 55–119. DOI: 10.5281/zenodo.22387

Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice

Cameron S. D. Brown[1]
Australian National University, Australia

Abstract

The primary goal of this paper is to raise awareness regarding legal loopholes and enabling technologies, which facilitate acts of cyber crime. In perusing these avenues of inquiry, the author seeks to identify systemic impediments which obstruct police investigations, prosecutions, and digital forensics interrogations. Existing academic research on this topic has tended to highlight theoretical perspectives when attempting to explain technology aided crime, rather than presenting practical insights from those actually tasked with working cyber crime cases. The author offers a grounded, pragmatic approach based on the in-depth experience gained serving with police task-forces, government agencies, private sector, and international organizations. The secondary objective of this research encourages policy makers to reevaluate strategies for combating the ubiquitous and evolving threat posed by cyber-criminality. Research in this paper has been guided by the firsthand global accounts (via the author's core involvement in the preparation of the Comprehensive Study on Cybercrime (United Nations Office on Drugs and Crime, 2013) and is keenly focused on core issues of concern, as voiced by the international community. Further, a fictional case study is used as a vehicle to stimulate thinking and exemplify key points of reference. In this way, the author invites the reader to contemplate the reality of a cyber crime inquiry and the practical limits of the criminal justice process.

Keywords: Agency, Anonymity, Attorney, Attribution, Capacity, Case, Cloud, Computing, Cooperation, Counsel, Court, Crime, Cross-Border, Cryptography, Cyber, Dark, Data, Decryption, Defense, Electronic, Encryption, Enforcement, Evidence, Expert, Forensics, Hack, Illicit, Information, Intelligence, Intercept, International, Internet, Investigation, Judge, Jurisdiction, Jury, Justice, Law, Lawyer, Legal, Liability, Monitoring, Net, Online, Order, Police, Policing, Policy, Privacy, Prosecution, Quantum, Proxy, Reporting, Security, Stalking, Surveillance, Sovereignty, Territorial, Threat, Transparency, United Nations, Universality, Web, Witness.

[1] Visiting Associate Investigator and Senior Research Officer - Australian National University | Information Security Professional - Cyber Defense, Strategic Intelligence, Digital Forensics, Incident Response | International Legal Practitioner - Public Policy Engagement, Governance, Data Privacy, Regulatory Compliance, Transactional Risk, Crisis Management, Evidence Authentication. Address: PO Box 328, Lorne VIC 3232, Australia. Email: cameron.brown@legalforensic.com

Introduction

With escalations in reports of serious cyber crime, one would expect to see a corresponding increase in conviction rates (Broadhurst, Grabosky, Alazab, Chon, 2014; Kaspersky Lab, 2015; Ponemon Institute, 2015). However, this has not been the case with many investigations and prosecutions failing to get off the ground (Frolova, 2011; Onyshikiv & Bondarev, 2012; Zavrsnik, 2010). The chief causes of this outcome may be attributed to trans-jurisdictional barriers, subterfuge, and the inability of key stakeholders in criminal justice systems to grasp fundamental aspects of technology aided crime. In the same way that science influences the utility of forensic inquiry, the capacity of investigators, prosecutors, judges and jurors to understand illicit use of technology also directly impacts conviction rates (Dubord, 2008; Leibolt, 2010). The ease with which cyber crime crosses national borders, irreconcilable differences between national legal frameworks, and deceptions employed by cyber criminals impedes attribution, and prevents crime fighters from interrogating suspects and apprehending offenders.

Cyber crime offending can be technically complex and legally intricate. Rapid advancements in the functionality of information communication technologies (ICTs) and innate disparities between systems of law globally are stark challenges for first responders, investigating authorities, forensic interrogators, prosecuting agencies, and administrators of criminal justice. It is critically important to explore factors impeding investigation and prosecution of cyber crime offending to raise awareness and expose these barriers to justice. This paper examines criminal justice responses to cyber crime under the common law model. The capacity of criminal justice actors to perform their core function is analyzed and discussed. The author contends that the investigation and prosecution of cyber crime offending, including forensic services in support of inquiries, is hampered by a confluence of factors that influence the criminal justice process. This thesis is illustrated with aid of a case study examining the criminal justice lifecycle throughout a cyber crime inquiry. Based on notorious instances of cyber crime offending, Mary's Case charts the initial commission of criminal activity through until the ultimate determination of culpability at trial.

This paper proposes a practical definition of cyber crime, which is linked to the impact of technology on modes of criminal offending. Victimology and impediments to cyber crime reporting are outlined. The common law model of criminal justice is surveyed, with a focus on the effect of both law and technology on policing cyber crime globally. Investigative techniques and operational challenges are discussed in detail. Evidentiary issues surrounding collection and presentation of electronically stored information (ESI) in criminal trials are evaluated. The key elements that coalesce to constitute serious criminal offending are deduced and contrasted with defenses to criminal capacity and culpability. The author also highlights issues concerning evidence admissibility, roles performed by lawyers, experts, and adjudicators during legal proceedings, and the media's influence upon public perceptions of forensic science. Finally, recommendations for removing barriers to the effectiveness of cyber crime inquiry are considered, including new strategies for streamlining the administration of criminal justice.

1. Criminal Activities Perpetrated Electronically

1.1. Defining Cyber Crime

Technical experts, police, lawyers, criminologists, and national security experts understand the concept of 'cyber crime' differently (Alkaabi, Mohay, McCullagh & Chantler, 2010). It is increasingly unclear whether cyber crime refers to legal, sociological, technological, or legal aspects of crime and a universal definition remains elusive (Kshetri, 2010). Analysts have attempted to frame the fundamental characteristics of cyber crime with limited consensus (Gordon & Ford, 2006; Snyder, 2001; Wall & Williams, 2001; Yar, 2005). Current definitions vary significantly, depending on the legal instrument or organization defining the term (Pocar, 2004). The abuse of ICTs by criminals is interchangeably referred to as cyber crime, computer crime, computer misuse, computer-related crime, high technology crime, e-crime, technology-enabled crime, amongst others (Goodman & Brenner, 2002). Yet, these terms are not synonymous (Chik & Bartholomew, 2011). Highlighting the extent of confusion and lack of consistency, the definition of 'e-crime' provided by the Association of Chief Police Officers (ACPO) is at odds with that provided by the Australian Institute of Criminology (AIC). According to the ACPO, "e-Crime" involves the "use of networked computer or Internet technology to commit or facilitate the commission of crime" (Association of Chief Police Officers, 2009). Contrastingly, the AIC regards "E-crime" as "A general label for offences committed using an electronic data storage or communications device" (Australian Institute of Criminology, 2011).

The semantics of 'cyber crime' point to a legal and technical phenomenon that proscribes criminal activity connected with the cyber domain. Such activity is categorically different to behavior deemed 'unethical' or 'against the law' which does not in itself amount to 'criminal conduct'. The author asserts that criminal justice processes should only be engaged when a course of conduct is determined to be truly criminal and warrants prosecution. Fundamental to most legal systems is the principle of '*nullum crimen sine lege*', meaning no matter how harmful the behavior, it cannot be prosecuted unless it is formally prohibited by law (Grabosky, 2007; Tikk, 2011). For the purposes of this research, the following elements must be present for an act to be classified as cyber crime offending:

- The conduct is facilitated *by information and communications technology;*
- The conduct is motivated by *intent* to commit *harm* against a *person* or *organization;*
- The perpetrated or intended harm encompasses conduct amounting to *interference* or *damage* to either *tangible* or *intangible property* owned by a *person* or *organization;* and
- The conduct concerned is *criminalized* within either the *jurisdiction of the victim* or the *jurisdiction of the accused*.

Under this definition, cyber crime is merely a sub-set of conventional crime where ICTs are used as a vehicle or tool to commit traditional criminal offences (Lupsha, 1996; Zhigang, 2011). This definition adheres to the rudiments of legal interpretation applied to traditional criminal offending. Legislators should be mindful to avoid creating '*sui generis*' legal categories of cyber crime offences by tailoring laws to meet changes in technology.

Instead, laws should be crafted to encompass technology broadly within established categories of criminal conduct.

Mary's Case: Cyber-Stalking

Mary is a student in her late-twenties attending a public university in Australia. After receiving a series of emails and instant messages containing sexually explicit comments she seeks help from her parents. Content within the messages indicates that the sender knows where Mary attends university, the people in her friendship circle, and other personal information. The identity of the sender is not disclosed in the correspondence. Concerned that the sender may be using personally identifiable information about Mary available on the Internet, her father performs online research. He discovers various comments mentioning Mary by name in postings on erotic websites, which appear to be hosted overseas. Nevertheless, both Mary and her parents are reluctant to report the matter, as they believe police lack the capacity to investigate crimes associated with the Internet and technology. Mary is also embarrassed about the content of the postings and maintains the incident is probably not serious enough for police to investigate.

1.2. Technology and Offending

Evidence in judicial proceedings is increasingly being stored, transmitted, or processed in electronic form. Technology has become the symbol, subject (place), tool (instrument), and object (target) of crime (Savona & Mignone, 2004). Although technology facilitates the commission of traditional crimes, including offences against property and offences causing personal harm (McQuade, 2006), existing national legal frameworks may be incapable of addressing evolving '*modus operandi*' related to cyber crime offending (Hughes, 2003). It is common for cyber crime to be transnational in terms of the physical location of victims, perpetrators, and evidence. The interconnectivity of the global economy enables criminals to operate trans-jurisdictionally, with discrete elements of their crimes speckled widely across the globe in both time and space (Herrera-Flanigan & Ghosh, 2010). Despite extra-territorial legal provisions for criminal acts perpetrated in foreign jurisdictions, the practical application of these laws is rather ineffective (Geist, 2003). Whilst an offender may be apprehended in one jurisdiction, the digital evidence required to progress an investigation may reside in another country (Scientific Working Group on Digital Evidence, 2000).

Trans-border elements are apparent in Mary's Case and accessing information stored in foreign jurisdictions complicates investigations significantly. Ultimately, cyber crime can be perpetrated inexpensively and easily, and victims are often left wondering if the offender is "half a block or half a world away" (Goodno, 2007, p. 129). The anonymity of cyber crime also increases the volume of offending and obstructs efforts to identify culprits, thereby distinguishing it from physical crimes (Brenner, 2008; Casey, 2004; Denning, 2001; Post, Ruby & Shaw, 2000). The disinhibiting effect of technology serves to psychologically distance criminals from the consequences of their victimizing behavior (Bocij & McFarlane, 2003; D'Ovidio & Doyle, 2003; Lidsky & Cotter, 2007). Moreover, purely text-based interactions may engender a false sense of intimacy, promote fantasy development (McGarth & Casey, 2002), and facilitate misleading and deceptive behavior due to reduced availability of sensory information (Finn & Banach, 2000; Spitzberg & Cupach, 2003). In addition to advanced technical aptitudes, cyber criminals have skills in linguistics and psychology, which they combine to execute social engineering deceptions,

manipulate decision-making processes, and distort perceptions (Chen, 2015; Holt, 2012; Mutnick & Simon, 2002; Waltz, 1998). In Romania, it is reported that cyber criminals engage native English speakers to give a veneer of legitimacy to online scams (Bhattacharjee, 2011). Compared to traditional criminal offending, cyber crime requires fundamentally different strategic and tactical responses from legislators, investigators, lawyers, and judicial officers (Wall, 2001).

1.3. Victimization and Reporting

The relatively anonymous and faceless nature of cyber crime complicates issues associated with victimology and cyber crime reporting (Bermay & Godlove, 2012). There exists widespread misunderstanding among communities about the nature of cyber crime and capacity of law enforcement to apprehend offenders. A number of factors impact the low proportion of cyber crime acts that are brought to the attention of police. Mary's Case is consistent with underreporting due to a lack of public confidence in the capability of police to investigate cyber crime offending (Collier & Spaul, 1992) There is also a widespread belief that law enforcement agencies are inflexible and intrusive (Davies, 1999; Walden, 2005; Wolf, 2000). Victims fear that prosecutors will not take on their case, or if they do, will publicize the case widely to raise the profile of the prosecutor or department concerned, without due regard to the impact of such publicity on the victim (Goodno, 2007; Herrera-Flanigan & Ghosh, 2010; Shafritz, 2001; Spitzberg & Hoobler, 2002). Many victims are also reluctant to come forward due to shame or the mistaken belief that the cyber crime incident is simply not serious enough to warrant police attention (United Nations Office on Drugs and Crime, 2013).

Cyber crime reporting is also impeded by a lack of awareness regarding reporting mechanisms (United Nations Office on Drugs and Crime, 2013). Identifying victims and perpetrators of cyber crime can be a very complex matter, and the disinclination of victims to come forward substantially impairs the capacity of police to respond. Widespread underreporting by Internet Service Providers (ISPs) indicates that new laws may be required to compel them to report suspicious activity on their networks (U.S. Department of Justice, 'A Review of the FBI's Investigations of Certain Domestic Advocacy Groups', 2010). Ultimately, the prevailing tendency for underreporting makes cyber crime offending increasingly less visible.

Mary's Case: Threats to harm

About a week after the initial contact, Mary informs her parents that she received a call from a stranger expressing interest in participating in 'sexual fantasies'. The caller claimed to be responding to an online message before he disconnected. Mary shows her parents a posting she found on an online bulletin board containing her name and phone number and a message broadcasting that she fantasizes about being raped. Mary subsequently receives an email message containing threats to harm her. Attached to the message are several photos depicting the house where she lives and images of her meeting with friends for coffee at university. There is also a photo showing an item of her clothing that she believes was taken from the clothesline. Mary and her parents report the matter to local police later that day.

2. Law Enforcement and Policing

2.1. The Common Law Model

Within the common law tradition, police play the leading role in the investigation of criminal activity and have significant independent powers (O'Connor, 2012). Typically, an investigation is commenced as soon as an alleged crime is brought to the attention of law enforcement personnel. Judges perform an integral oversight function during investigations, particularly where police activity interferes with the rights of suspects or other individuals (Hodgson, 2010). The requirement for police to obtain a warrant from a judge theoretically ensures that individual rights are given judicial consideration as police seek to move ahead with an inquiry.

Police are responsible for interviewing suspects, victims and witnesses. The information gathered is usually assembled in the form of a brief or case file. For lesser offences, police can charge the accused and present the case in court. For those instances, involving the commission of serious criminal offences, the police will collaborate with a prosecutor who assumes chief responsibility for deciding which charges are appropriate, if any. Whilst police are responsible for collecting and securing evidence, in some common law countries the prosecutor may advise police during the evidence-gathering phase. It is the role of the prosecutor to present the charges to the court for confirmation and approval.

In the common law tradition, defense counsel performs an active role by advising clients during police interviews and acting on their behalf. During the investigative phase, defense counsel can gather evidence independently and hire expert witnesses. Due to the adversarial nature of the common law system, the defense is given full access to the case file and must be afforded reasonable opportunity to examine all evidence in advance of trial. A process of 'discovery' or 'disclosure' is the formal legal mechanism regulating the sharing of evidence between the defense and prosecution (O'Connor, 2012).

There are complex rules related to admissibility of evidence (Thaman, 2013). As the trial unfolds, the chief protagonists are the prosecutor and defense counsel. The judge functions as an impartial referee between the parties and is tasked with instructing the jury on matters of law (Acharya, 2003). The common law trial can be a lengthy process, as witnesses are typically required to deliver their evidence via 'live testimony' before the court (O'Connor, 2012). Initially, the witness is examined by the party calling them. This is also referred to as 'examination-in-chief'. The witness is then cross-examined by the other party, after which the party calling the witness has the opportunity re-examine the witness again. This process continues until all witnesses have delivered their testimony (Parker & Kobayashi, 1999). In theory, the drive to win encourages each party to carefully examine the evidence and lead persuasive argument in support of their case. Ideally, the truth emerges as the judge or jury observes the proceedings.

A key issue with this model is that the capacity to discover evidence is usually tied to the resources of the opposing parties, which may be unequal. Ultimately, each party is entitled to the best representation that they can afford. The ease of access to forensics facilities for policing agencies stands in stark contrast to the expense of engaging forensic support for many defendants. This inequity is regarded by some as "an economic presumption of guilt" (Kelly & Wearne, 1998, p. 15). The danger here is that sources of exculpatory evidence may not be revealed due to investigative bias among criminal justice

officers, who ultimately decide what tests are performed and which aspects of the forensic evidence is reported upon (Zonderman, 1999).

2.2. Legal Frameworks, Police Mandates and Policy

Despite the valiant efforts of the Council of Europe (CoE), Interpol, Europol, the European Union (EU), the Organization for Economic Cooperation and Development, the G8 Group of States, and the United Nations (UN), amongst others, much work is needed to regulate international dimensions of cyber crime. Although the *CoE Convention on Cybercrime* (2001) and the *Additional Protocol* (2003) (hereinafter referred to as the *Budapest Convention*) has been signed and ratified by non-member states, it is largely a product of regional collaboration, reflective of conditions and premises among CoE Member States. As of August 2015, only 47 nation-states had ratified the Convention (Council of Europe Treaty Office, 2015). Unsurprisingly, various provisions within the *Budapest Convention* are considered a threat to state sovereignty by pockets within the international community. Russia's National Coordinator for the Shanghai Cooperation Organization (SCO) described the *Budapest Convention* as less than satisfactory, and in violation the Russian Constitution by permitting foreign law enforcement agencies to conduct investigations within Russian borders via the Internet (Kizekova, 2012).

In 2011, Russia, China, Tajikistan and Uzbekistan submitted a draft of the *International Code of Conduct for Information Security* before the 66th UN General Assembly Meeting (United Nations General Assembly, 2011). The Code seeks observance of human rights and freedoms within the information space (Brown, 2015). Respect for the sovereignty, territorial integrity and political independence of all nation-states is also addressed, and the code pushes for the development of transparent multilateral and democratic international Internet governance arrangements (Kshetri, 2013). In 2015, Secretary of State John Kerry affirmed the view of the US during remarks made to an audience in South Korea. He stated that "basic rules of international law apply in cyberspace" and "countries should work together to deter and respond effectively to online threats" (U.S. Department of State, 2015). He also promoted the *Budapest Convention* as "the best…legal framework for working across borders to define what cybercrime is and how breaches of the law should be prevented and prosecuted" (U.S. Department of State, 2015).

However, without a universal cyber crime convention, cross-jurisdictional conflict of criminal laws raises the unavoidable dilemma of "what law should be applied to determine the legal effect of a person's conduct when he does an act in one state which produces harmful effects in another" (Stimson, 1936). Cyber crime cases that demand cooperative mechanisms that are not provided for within existing legal instruments create significant difficulties for police and prosecuting agencies (Bermay & Godlove, 2012; Gercke, 2012; International Telecommunications Union, 2012). The following multilateral and bilateral instruments are only able to deliver solutions within certain contexts:

- *Budapest Convention*;
- *United Nations Convention against Transnational Organized Crime* (2000) and its three protocols;
- *European Convention on Mutual Assistance in Criminal Matters* (1959);
- *Inter-American Convention on Mutual Assistance in Criminal Matters* (1992);

- *Stanford Draft International Convention to Enhance Protection from Cyber Crime and Terrorism* (1999);
- *Draft African Union Convention on the Establishment of a Credible Legal Framework for Cyber Security in Africa* (2011); and
- *Commonwealth Model Law on Computer and Computer Related Crime* (2002).

When police receive an incident report at the local level, a number of conditions must be met before a formal investigation can be initiated. To have the requisite jurisdiction, the type of behavior, which forms the substance of the report, must be regarded as criminal conduct under the national legal framework concerned. In other words, the police must determine which criminal law has been violated, if any (Goodman & Sofaer, 2001). The '*principle of territoriality*' in international criminal law holds that a crime committed within the territory of a nation-state may be tried there. Yet, in a networked world, the territoriality of criminal law does not always coincide with territorial sovereignty (Cassese, 2001). "While with physical crimes, such as in murder, the…elements are generally concurrent, with information-based criminal activity, such as in cybercrime, a jurisdictional distinction between the initiation and termination of an act becomes the norm" (Walden, 2003, p. 295). As such, an act may be initiated in one jurisdiction and the effect or harm felt in another.

Many cyber crime offenders have evaded prosecution due to weaknesses in substantive criminal laws that do not address technological means of offending (Downing, 2005). Determining the place where an offence was committed (*locus delicti*), and overcoming positive and negative conflict of laws can present difficulties for police, prosecutors and judicial officers when issuing warrants, drafting subpoenas, and committing a case for trial (Brenner & Koops, 2004). Compared to serious violations of human rights, many acts of cyber crime do not invoke the '*principle of universality*' as grounds for criminal jurisdiction (Broadhurst, 2006). Doctrines enshrined in one legal system may not impose obligations in foreign jurisdictions. The "sovereign equality" existing between nation-states is a fundamental principle of international law, which demands respect for the lawmaking autonomy of other countries (Roth, 2005, p. 1). Ultimately, criminal law is simply a tool for targeted governance and protection of public mores within a specific locality.

Whilst not an offence in itself, cyber stalking in Mary's Case would be covered by statutory provisions associated with stalking in Australia. However, any inconsistency in defining the constituents of crime among nation-states can be problematic. For example, in some countries there are no laws criminalizing possession and distribution of child pornography (Commonwealth Internet Governance Forum, 2012), and cyber-stalking legislation in some jurisdictions requires that a credible threat to the victim be substantiated (Schwartz, 2009). In order to address trans-jurisdictional cyber crime offending, international legal frameworks must be harmonized (U.S. Department of Justice, 2009). However, enacting legislation and ratifying treaties is a slow process compared to the rapid uptake of new technologies by diverse communities globally.

Police function to reassure the public, reduce crime, investigate crime, provide emergency services, maintain peace and order, and safeguard the security of the state (Bowling & Foster, 2002). These undertakings seek to fulfill fundamental police mandates targeting community safety and support, criminal and disorder control, and provision of services for the administration of criminal justice (Broadhurst & Davies, 2009). Yet,

policing is not just about exercising the powers of government. The remit encompasses a process "whereby social order and regulation is maintained" to ensure social happiness (Findlay, 2004, p. 4). Strategic and tactical methods of policing involve competing objectives that are a source of conflict for law enforcement agencies (Luen & Al-Hawamdeh, 2001). There are both extrinsic and intrinsic challenges associated with identifying targets and a tendency exists to concentrate, for ideological or practical reasons, on suspects most often involved in a particular type of criminal activity (U.S. Department of Justice, 2010). Bureaucratic obstacles and the politicization of policing can lead to direct and indirect pressure from senior governmental figures to reach a desired outcome congruent with an existing policy preference (Gill & Phythian, 2012). Consequently, police are less likely to commit time and money to investigate offences that do not present as an important public priority (Banks, 2010). Historically, this has been the case with cyber crime offending (Goodman, 1997).

Policing institutions also engage in self-preservation and image building to ensure their survival (Broadhurst & Davies, 2009). To operate efficiently, police must engender and maintain positive perceptions about their function and the quality of work that they perform. This includes managing public attitudes concerning the capacity of police to provide community safety and security. A perceived need to 'measure up' often compels police to take on unmanageable workloads or promise results that may be very difficult to deliver. Compared to traditional criminal investigations involving discrete face-to-face interactions between humans, cyber crime offending is associated with voluminous data, which must be processed to extract sources of evidence. Law enforcement agencies worldwide are overwhelmed by the prevalence of cyber crime cases (Maher, 2013). Extensive case backlogs have prompted some agencies to abandon investigations altogether. For example, the FBI is reputed to shy away from investigations unless quantified loss or damage meets the minimum threshold of US$5,000 (Akin, 2011, p. 751). In the same vein, the Case Acceptance Criteria for the Police Central e-Crime Unit in the UK targeted only "the most serious e-Crime incidents" and would not investigate instances of cyber-stalking (ACPO, 2009, p. 8). Many law enforcement agencies are also reluctant to pursue cyber crime cases at the local level as perpetrators mostly target victims in foreign jurisdictions (Kshetri, 2013).

Mary's Case: Police Report

Upon receiving the report, the local police refer the matter to the specialist e-Crime Unit. Senior Constable Lyon is tasked with investigating the case. Given the immediacy of the threats perpetrated against Mary, the matter is given 'high priority' status. Lyon contacts Mary and arranges to meet for an interview. During the interview, Lyon obtains copies of all electronic correspondence between Mary and the stalker, including data residing on her computer and handheld devices. Lyon warns Mary that it can be difficult to investigate cyber-stalking, particularly if the stalker or the evidence is located in another country. He pointedly asks Mary if she has recently had a "falling-out" with anyone or has any suspicions concerning the identity of the offender. Mary tells Lyon that she had a "bad break-up" with a former boyfriend upon discovering him cheating with one of her friends.

3. Investigating Cyber Crime

3.1. Mindset and Technical Competencies

Even with strong substantive and procedural domestic criminal laws and assent to international instruments such as the *Budapest Convention*, investigations may yield little unless police are well equipped and competent. A major task faced by the broader criminal justice community is communicating a shared understanding regarding the main technical skills, knowledge and roles performed during investigations and prosecutions (Graycar, 2001). Many cyber crimes are sophisticated and well-conceived, requiring police to apply technological expertise and deductive reasoning to unravel complex '*modus operandi*' and substantiate elements of an offence (Bromby, 2006). Information security's emphasis on hardware and software solutions for monitoring traffic and securing data is wholly inadequate when pitted against innovative blended attack vectors (Ghosh, 2002). Organized and persistent cyber-attacks have circumvented security precautions within major global corporations and stolen information and money with relative ease (Robertson, Riley, Strohm & Chan, 2014). Advanced blended attacks leverage vulnerabilities in fixed and wireless networks to steal credentials and conduct reconnaissance (FireEye Labs, 2015). Criminals use behavioral profiling to masquerade as ordinary system users whilst navigating private networks and exploiting applications to avoid arousing suspicion (CrowdStrike, 2015). Ultimately, signature-based commercial solutions lack the intelligence needed to identify and neutralize persistent nefarious activity that moves laterally and quietly (Brown, 2015).

The idiom 'rubbish in, rubbish out' reflects the danger of appointing untrained and incapable personnel to capture proof of malevolent activity and secure evidence of cyber crime offending. Seasoned leadership is required to effectively direct investigations and supervise the provision of forensic support (Horswell, 2004; Raymond, 2006). Unfortunately, bureaucrats with little in the way of technical background, often fill leadership positions in government, police, and law enforcement agencies within these areas. Like the organized criminal elements that embrace new technologies whilst adhering to proven techniques for committing crime, investigators must think like their criminal adversaries to decipher the technical underpinnings of cyber crime offending (Endgame, 2015; Nuth, 2008). Crime scene examiners are the lynchpin of successful investigations and the critical first step for initiating the chain-of-custody (Stanley & Horswell, 2004). Technology improves the capacity of police to capture a vast array of potential evidence (Mandel, 1987), but it is the human side of a cyber crime inquiry which is pivotal for giving meaning and weighing significance of ESI. Police must interpret and correlate information to support case theories and pursue leads by initiating dialogues with key individuals that are central to an investigation. It is critical for law enforcement agencies to retain personnel with this investigative mindset to expose cyber crime offending. Aside from electronic evidence, investigators also draw on other forensic science disciplines to gather physical trace evidence from crime scenes, including print, hair, and fiber artifacts (Gilbert, 2004; Kaye, 1995; White, 2004).

Skilled investigators in the digital domain possess a natural sense of curiosity combined with a desire to clarify the truth, establish facts, and reveal the answer to technical questions that arise during an inquiry. Deductive and inductive reasoning is employed to establish sequences of events. Traditional law enforcement techniques including

surveillance, interviewing, search and seizure, and formal legal process mechanisms are then implemented to support or refute case theories. This combination of skills goes beyond basic protocols of 'bagging-and-tagging', or 'monkey see, monkey do'. The aptitude is one of connecting pieces of information to form general rules or conclusions, as well as identifying relationships among seemingly unrelated events. As a case unfolds, core methodologies are attuned to address specific challenges as investigators rely on intuition and fluidity to pursue leads (Horswell, 2004; Robertson, 2004). As such, the investigative mindset is an adaptive approach to solving problems based on understanding the source material, preparation and planning, analysis, collation and recording, and assessment. The aim "is to develop disciplined approaches to decision making and to ensure all decisions are relevant, appropriate and can be demonstrated to others" (Hunton, 2011, p. 62).

Yet, despite the pervasiveness of digital information, many police and prosecutors are hesitant to collect and present intangible sources of evidence. Lack of leading edge tools and shrinking budgets for procuring resources are ongoing problems (Mislan, 2010). Finding the right blend of competencies to meet the rigors of a cyber crime inquiry is very difficult. The blend of investigative and technical methodologies employed by digital forensics interrogators is derived from scientific knowledge and practical knowledge from repeated casework. Although forensic analysis can uncover the 'smoking gun' which makes or breaks a case, more often it adds value by providing intelligence to establish facts of a corroborative nature (Saferstein, 1983). The need for trained investigators and prosecutors who are conversant with sources of electronic evidence is becoming increasingly critical as criminal acts move from physical to digital domains. In order to effectively attend to the rigors of a cyber crime inquiry, investigators require a range of 'soft' and 'hard' skills, coupled with the experience to apply those skills in real and virtual environments (see *Table 1* and *Table 2*).

Table 1. Soft Digital Forensics Investigative Skill Sets

Soft Skill	Competency
Communicative	Liaise with the public, other team members, court staff, lawyers, law enforcement personnel, and other interlocutors.
Rational	Swiftly assess a situation and make appropriate decisions.
Collaborative	Rapidly gain the confidence of others and sustain those relationships.
Intuitive	Instinctively differentiate between normal and abnormal events.
Coherent	Explain technical subject matter in plain language and make information accessible to diverse audiences.
Resilient	Prioritize and maintain composure whilst working under pressure.
Punctual	Meet deadlines and provide deliverables to specification.
Fastidious	Maintain focus with persistent attention to detail.
Disciplined	Restrained work ethic with strict observance to directives and mindfulness of personal and technical limitations.
Strategic	Formulate and ask probing questions to key stakeholders and devise plans, which bring value to an inquiry.

Table 2. Hard Digital Forensics Investigative Skill Sets

Hard Skill	Competency
Research	Expeditious retrieval of information in the public domain and reference material stored across the corporate network. Capacity to gain insights by triangulating information from disparate sources that are inaccessible via public search engines.
Awareness	Vigilance in maintaining awareness of developments in the field of information security. Applied knowledge of industry best practices for conducting digital forensics investigations.
Evidence Continuity	Strict compliance with established processes for demonstrating chain-of-custody when handling electronically stored information.
Forensic Imaging	Applied knowledge of data preservation techniques, which use both physical and logical methods to forensically acquire data and verify sources of information.
Networking Architecture	Practical understanding of the Open System Interconnection (OSI) model and the function of communication technologies in the storage and transmission of data, such as network protocols, media access control (MAC) addresses, firewalls, routers, proxy servers, data centers, online applications, cloud services, host-based applications, redundant array of independent disks (RAID), clusters, virtual servers, and modes of multifactor authentication.
Hardware	Applied knowledge of components and peripherals connected to information systems, including hard disk drives, solid state drives (SSDs), random access memory (RAM), the basic input output system (BIOS), network interface cards (NICs), chipsets, and flash storage.
File Systems	Applied knowledge of diverse file system attributes such as FAT, FAT32, exFAT, NTFS, HFS+, XFS, Ext2, Ext3, Ext4, and UFS.
Structured Data Analysis	Retrieval and interpretation of universally formatted information, such as fixed field entries inside records, as well as embedded information associated with operating systems, relational databases, spreadsheets, registries, Internet history, security and system logs, and encrypted file systems.
Unstructured Data Analysis	Interpretation of values associated with detached files stored across various file systems such as digital photos, graphic images, videos, streaming data, webpages, PDF files, PowerPoint presentations, email data, blog entries, wikis, and word processing documents.
Semi-structured Data Analysis	Extraction of tags, metadata, or other types of identity markers subsisting within detached files, including information indicative of authorship, revision number, creator, sender, recipient, time and date particulars, GPS coordinates, keywords, and firmware version. This activity also extends to analysis of relational data within files that are associated with detached files, such as XML and other markup languages.
Reverse Engineering	Functional understanding of the mechanics of software development, remote administration, and malware proliferation.
Programming and Scripting	Knowledge of coding using languages such as C, C++, C#, Perl, Delphi, Html, .NET, ASP, Python, Java, JavaScript, Ruby, Bash Scripting, VBScript, PowerShell, Unix/Linux, EnScript.
Virtualization	Applied knowledge of building, configuring, and deploying virtual machines.
Technical Reporting	Experience in producing highly granular reports detailing the inner workings of information communication technologies, file integrity, authenticity of information, and movement of data.

3.2. Search and Seizure

Cyber crime investigation may involve some form of invasive or coercive search, surveillance, or monitoring activity by law enforcement or intelligence agencies (O'Harrow, 2005; Stephenson, 2003; Zavrsnik, 2010). Search and seizure is an active

mode of investigation, which involves discovering evidence, identifying suspects, apprehending offenders, and interviewing witnesses. Legal authority and best practices for executing search and seizure warrants varies considerably between jurisdictions and criminal justice systems, including rules governing handling electronic evidence (Jarrett & Hagen, 2009; United Nations Office on Drugs and Crime, 2013). When police conduct search activities, hardware, software, peripheral storage devices, and information in binary and printed form may be seized. It is incumbent for investigators to consider the appropriateness of previewing and forensically acquiring data at the scene (i.e., *'in situ')* and whether the circumstances may justify physically seizing equipment for further analysis in a laboratory (Clancy, 2011).

In most western democracies, national legislative provisions exist to enforce compliance with international human rights law, including the rights to privacy and freedom of opinion and expression. For example, articles 10 and 17 of the *Universal Declaration of Human Rights* (1948), article 6 of the *European Convention for the Protection of Human Rights and Fundamental Freedoms* (1953), article 16 of the *Convention on the Rights of the Child* (1989), article 22 of the *Convention on the Rights of Persons with Disabilities* (2006), article 14 of the *Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families* (1990), article 8 of the *European Convention on Human Rights* (1950), article 11 of the *American Convention on Human Rights* (1969), and articles 10 and 17 of the *International Covenant on Civil and Political Rights* (1966) to which 168 States are party. Even in instances where UN Member States are not bound by a treaty or convention, these instruments present minimum standards and are reflective of customary legal norms. As such, nation-states that have signed, but not ratified an instrument, are bound to respect its purpose and object, in accordance with article 18 of the *Vienna Convention on the Law of Treaties* (1969). However, customary legal norms have certainly lost some of their potency in recent years, particularly with respect to their applicability to cyberspace (Brown, 2015). For example, the articles 2(4) and 51 of the *Charter of the United Nations* (1945) cannot necessarily be relied upon to give staunch guidance to policy-makers globally regarding data driven hostilities (Schmitt, 2013). Nevertheless, national legal frameworks also exist to protect privacy, opinion and expression (e.g., section 13 of the *Charter of Human Rights and Responsibilities Act*, 2006, Victoria).

Prior to commencing a search, investigators must ensure that they abide by applicable laws or risk having seized exhibits declared inadmissible at trial. In some jurisdictions there are exceptions that may justify warrantless search and seizure activities (e.g., consent, 'emergency' terrorist situations, plain view doctrine, search relating to arrest, etc.) but an actual search of the data stored on a device usually requires a warrant in common law countries. In circumstances where there is a substantial risk of losing evidence, such as where data sanitizing and other anti-forensics tools are active, some jurisdictions permit law enforcement to perform a limited search of devices without a warrant due to the perceived vulnerability of the data (Dee, 2012). Remote wiping and deletion tools are bundled preinstalled on many mobile devices and available for purchase as commercial software or freeware. During warrant activity, investigators may also discover legally protected sources of ESI (e.g., doctrine of legal professional privilege, public-interest immunity, etc.), adding a layer of complexity to the process of evidence handling. Many investigators encounter administrative delays in obtaining legal authority to conduct police investigations due to judicial uncertainty about cyber crime offending. Albena Spasova, who worked in promoting law reform in Moldova and Bulgaria, commented: "Even in

2001, I was meeting judges who thought cyber-crime was someone stealing a computer" (Kshetri, 2013, p. 10).

3.3. Stored Communications

During the course of an investigation, police usually gather information about an event after it has occurred. The re-enactment of cyber crime offending requires investigators to trace communications back to a source and retrieve information about that communication (Herrera-Flanigan & Ghosh, 2010; Schjølberg & Ghernaouti-Hélie, 2011). The capacity of police to identify individuals in control of domain names and Internet Protocol (IP) addresses at a given point in time is a fundamental step in the investigative process (U.S. Department of Justice, 'Investigations Involving the Internet and Computer Networks', 2007). Investigators with the requisite legal authority and related information about a suspect (e.g., username, IP address, time and date of suspicious activity) may also be able to obtain subscriber data, transactional or traffic data, and content data from service providers (Australian Government, 2012). Investigators are more likely to establish a link between a suspect and the commission of crime if they can secure data from physical devices used by a suspect to corroborate subscriber, transactional and content data. Article 1d the *Budapest Convention* defines "traffic data" as "any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service" (Convention Committee on Cybercrime, 2001). 'Content data' is not defined in the *Budapest Convention* "but refers to the substance of the communication, that is, the meaning of the communication, or the message or information being conveyed (other than traffic data)" (Broadhurst, 2006, pp. 408-433).

In some jurisdictions, telecommunications providers can supply investigators with stored content such as voice mail, call logs, and codes for accessing data contained on Subscriber Identity Module (SIM) cards by leveraging Pin Unlock Key (PUK) codes for handsets (Nelson, Phillips & Steuart, 2010). Police may also trace phones in real time through the telecommunications network using cell tower data in combination with geospatial technology (e.g., Stingray) which may also be programmed to match phone signals and voice prints (Boyle, 2007; Farivar, 2015; Lichtblau, 2012; Van Brocklin, 2014). *Table 3* presents examples of subscriber, transactional, and content data that police commonly target during an investigation. Yet, the abundance of telecommunications carriers can make it extremely difficult to trace a single communication, as multiple legal processes are potentially required to simply establish origin. Business models related to retention and storage of data also differ regionally. Oftentimes, police are able "to successfully trace one or two steps, only to find out that an upstream carrier has not retained the information, which is critical to continue the investigation" (Herrera-Flanigan & Ghosh, 2010, pp. 305-306). The problem for law enforcement concerns "practical difficulties in intercepting the communications and related data that courts have authorized it to collect" (Caproni, 2011). Some service providers are even reluctant to allow police access to basic information about a user, thereby further thwarting investigations. There is manifest disagreement among ISPs in many jurisdictions concerning the legal process that police must follow to obtain subscriber data. Simply obtaining Internet account information for a single user can be "complicated and involve an increase in the amount

of paperwork and time an investigator spends on a case" (D'Ovidio & Doyle, 2003, p. 15.).

> What this means is that an order from a judge to monitor a suspect's communication may amount to nothing more than a piece of paper. Some companies fail to comply with the court order. Some can't comply, because they have not developed interception capabilities. Other providers want to provide assistance, but they have to build interception capabilities, and that takes time and money (Comey, 2014).

Table 3. Service Providers and Avenues of Inquiry for Investigators

Subscriber Data	Traffic/Transactional Data	Content Data
Name and address	Connection logs detailing dynamic or static IP addresses assigned by the service provider and Uniform Resource Locators (URLs)	Stored electronic communications retrieved from remote computing services (e.g., email messages, SMS/MMS messages, pagers messages, voice mail, video messages)
IP address used to register an account		
Telephone number	Account usage logs reflecting IP addresses accessed via a subscription service	Stored electronic communications from remote computing services not yet retrieved (e.g., stored fax messages, synchronized data associated with cross-platform applications)
Email address		
Credit card particulars, direct debit account details, or other method of payment	Information exchanges processed through a service provider (e.g., email header information, records of shared folders)	Records of financial transactions stored in online banking accounts and payment facilities (e.g., PayPal) including records of transfers using digital currencies (e.g., Bitcoin wallets)
Service agreement information (e.g., commencement date)		
Geographical location of a service	Records of wireless carrier services pointing to the location of a subscriber's device (e.g., triangulation of cell tower data, GPS coordinates)	Data uploaded, downloaded or shared via cloud services (i.e., platform as a service, infrastructure as a service, software as a service, network as a service)
Internet connection records (e.g., quantity of data downloaded and/or uploaded)	Itemized records logging usage (e.g., numbers dialed, time and date of calls, communication logs)	
Time and duration of service usage (e.g., session times, calls and/or connections)	Information identifying the sender and recipient, including copy recipients, for a communication (e.g., email header information, shared folders, attachments)	Managed and automated backup services for computers and mobile devices (e.g., iCloud, OneDrive)
Use of subscription-based telecommunications services (e.g., conference calling, call messaging, call waiting, call barring, call forwarding, call redirection, calling line identification services)	Routing information identifying equipment through which a communication is, or has, been transmitted (e.g., dynamic IP address allocation, file transfer logs)	Data hosted in datacenters and cloud computing environments (i.e., private, community, public clouds, hybrid clouds)
Use or selection of preferential numbers or discount calls		
Connection, disconnection and reconnection of services	Addresses or other markings written on, or associated with, a postal item (e.g., names, telephone numbers, tracking numbers)	User data associated with social networking platforms (e.g., screen names, contact lists, multimedia, documents, messages, postings)

The possibility of obtaining information from an ISP naturally depends on police having legal authority to make such a request and there being adequate data retention and logging policies in place. The ephemeral nature of user logs and the "financial and human costs associated with gathering and maintaining account information decreases the

possibility that Internet service providers will voluntarily collect and maintain such data for a useful period of time" (D'Ovidio & Doyle, 2003, p. 15.). In the absence of universally agreed standards concerning data retention, investigators often discover sources of ESI vanishing as logs are overwritten and data records are purged to free space. Whilst investigators may be able to compel an ISP to freeze or preserve stored data, the issue of data retention remains very controversial (Schjølberg & Ghernaouti-Hélie, 2011). The European Court of Justice held that Directive 2006/24/EC of the European Parliament and of the Council (i.e., Data Retention Directive) is invalid and a violation of the *Charter of Fundamental Rights of the European Union* (2000) for exceeding limits imposed by the principle of proportionality.

> It entails a wide-ranging and particularly serious interference with the fundamental rights to respect for private life and to the protection of personal data, without that interference being limited to what is strictly necessary...[B]y requiring the retention of those data and by allowing the competent national authorities to access those data, the directive interferes in a particularly serious manner with the fundamental rights to respect for private life and to the protection of personal data (Court of Justice of the European Union, 2014).

3.4. Monitoring and Interception

Some national legal frameworks empower police and security agencies to obtain court orders to intercept communications between computers in urgent and exceptional cases. The *Code of Criminal Procedure* (2000) in France includes a power to requisition documents relevant to an investigation including the transfer and conversion of computer data, the decryption of computer data, wiretapping, and the interception of other communications (e.g., Articles 706-35, 706-47, 706-81, 227-18, and 227-24). This legislation also provides a legal basis for the activities of law enforcement agencies engaged in online investigations. This power extends to monitoring persons suspected of committing a crime when law enforcement officers gather evidence by posing online as criminal accomplices or receivers.

'Real-time' digital monitoring activities, also called 'tapping' and 'bugging', can be facilitated with use of covert software and hardware tools, which, once installed, enable access to devices in possession of suspects (Downing, 2005; Gill & Phythian, 2012). Live interception techniques also allow investigating authorities to capture transmissions as they are sent and received. For example, the *Regulation of Investigatory Powers Act* (2000) (RIPA) provides law enforcement agencies in the UK with the power to:

- Intercept communications (i.e., traffic and content data);
- Conduct 'intrusive surveillance' (i.e., covert in private premises or vehicles, etc.);
- Conduct 'directed surveillance' (i.e., covert in a public place);
- Use covert human intelligence sources (i.e., undercover agents); and
- Monitor communications data (e.g., records related to communications but not the content of such communications, etc.).

Once a suspect device has been identified, investigators may deploy a variety of technologies to harvest intelligence. For example, system activity may be recorded using

'Remote Administration Tools' (RATs), keyboard entries monitored using keystroke loggers, cameras installed to capture passwords and physically link activity with a specific user, and 'packet sniffers' activated to intercept communications and gather information about a particular network. Whilst conventional investigative powers prohibit remote searches beyond the local jurisdiction, it can be very difficult to determine when data crosses international borders (Chong, 2012). The legal treatment of data may differ significantly from one country to another, posing a minefield of technical and legal complexities. As such, it becomes critical that investigators and prosecutors be well-informed of geo-specific data-mapping issues and maintain vigilance in observing legislative changes globally, including the imposition of sanctions and embargoes between nation-states (Vincent & Hart, 2011). Managing dual criminality provisions for extradition, processing requests for mutual legal assistance (MLA), and balancing sensitive diplomatic relations are all significant encumbrances for investigations into cyber crime offending.

Even where strong diplomatic ties exist, underdeveloped states are unlikely to have adequate investigative powers or resources to assist cross-border investigations (United Nations Office on Drugs and Crime, 2012). To overcome these hurdles, some nation-states have enacted legislation with extraterritorial reach to empower domestic law enforcement agencies to remotely access data stored in foreign jurisdictions (i.e., 'online inspection') (Sieber, 2012). However, the international community has expressed concern about these encroachments on state sovereignty (Brown, 2015).

3.5. Proactive Strategies

Many law enforcement agencies have developed specialized units that target offenders online through social networking websites, chat rooms, instant messaging platforms, cloud services, Darknet forums, and other peer-to-peer communicative mediums (Dubord, 2008; Mitchell, Wolak & Finkelhor, 2005). Undercover operatives conducting online investigations use the ruse of impersonation in an attempt to build trust from targeted suspects. In many cases, online investigations are initiated further to complaints received from parents in circumstances where someone has contacted a child online and is behaving inappropriately (Tetzlaff-Bemiller, 2011). Such investigations are reactive and may involve an undercover officer taking control of a child's online identity to discover more about the intentions of a suspect (Mitchell, Wolak & Finkelhor, 2005).

By interacting directly with suspects, investigators are able to witness offences as they occur and need only wait for perpetrators to reveal themselves (Girodo, Deck & Morrison, 2002, Tetzlaff-Bemiller, 2011). For the most part, this type of undercover work targets criminals involved in child sex solicitation and abuse. However, with the emergence of highly organized online criminal marketplaces (e.g., Silk Road) the scope of online offending is now vast (e.g., drug trafficking, contract killing, trading in stolen credit cards, malware distribution, money laundering, etc.) (e.g., *United States v Ross William Ulbricht*, 2015) (Lusthaus, 2013). Investigators engaged in undercover operations require a comprehensive understanding of the laws governing engagement with suspects to ensure the admissibility of evidence and credibility of admissions (e.g., entrapment, inducement, etc.) (Ballin & Ballin, 2012). Proactive investigations of this nature often succeed because the problem of attributing criminal activity online also makes it very difficult for offenders to identify undercover agents (Lusthaus, 2012).

Mary's Case: Investigative Hurdles

A short time after the interview with Mary, Lyon meets with the Officer-In-Charge (OIC) of the e-Crime Unit to deliver a progress report. Lyon tells the OIC that he has traced the Internet postings vis-à-vis Mary to an adult website hosted in Moldova and a public classifieds forum hosted in the US. Upon request, the service provider in the US removed the offending material and forwarded data associated with the posting, but this data produced no value as the recoded IP address pointed to use of an anonymizing proxy service. The entity in Moldova flatly refused to cooperate. The email and instant message communications also yielded nothing as the sender stripped email header information using a remailer service in Serbia, and SMS records were concealed by routing messages through a satellite-based telephony service in Russia. The Serbian and Russian service providers were likewise uncooperative. The OIC then enquires about the outcome of the digital forensics inquiry. Lyon explains that the Victim's devices have not been forensically examined due to an extensive backlog of cases also requiring urgent attention.

Table 4. Use of Digital Forensics in Civil and Criminal Investigations

Civil Investigations	Criminal Investigations
Unauthorized access to information systems	Fraud
Unauthorized data duplication	Insider trading
Industrial espionage	Possession of prohibited material
Termination of employment	Theft of intellectual property and trade secrets
Breach of contract	Stalking and threatening behavior
Breach of corporate policy	Sabotage of information systems
Harassment in the workplace	Theft of property and assets
Bankruptcy and insolvency	Counterfeit and forgery
Due diligence inquiries	Assault and sexual offences
Loss of inventory	Homicide
Disclosure of personally identifiable information	Drug trafficking
Negligence	Money laundering

3.6. Crime Scene Processing and Forensic Services

Policing has been revolutionized by digital forensics and the development of specialized tools to aid investigative processes into cyber crime offending (Leibrock, 2008). As a scientific field of endeavor, forensic science uses technology to assist in the establishment of facts by a court of law. Digital forensics is a branch of forensic science, which encompasses the discovery, acquisition and investigation of information associated with digital devices. Originally used as a synonym for computer forensics, the term digital forensics has expanded to involve the investigation of any device capable of storing information in digital form. Digital forensics investigations have a variety of applications and the use of forensic techniques in the digital domain is increasingly an essential element of high-tech investigations, but also to support or refute the theory of a case in traditional

civil and criminal investigations (see *Table 4*). "As a forensic discipline, nothing since DNA technology has had such a large potential effect on specific types of investigations and prosecutions as computer forensic science" (Noblett, Pollitt & Presley, 2000).

Table 5. Discoverable Information during Digital Forensic Investigations

Storage Mediums	Electronic Information
Hard Disk Drives (HDD)	Firmware information | Basic Input Output System (BIOS) | Registered ownership and software registration information | Log entries |Metadata | Operating system registers | Media Access Control (MAC) addresses | IP addresses | Service Set Identifiers (SSID) | Information associated with network peripherals (e.g., Address Resolution Protocol, Routing tables, Network Address Translation, Access Control lists, etc.) | Temporary files | System files | Passwords | Deleted files | Hidden files | Compressed files | Encrypted volumes | Encrypted archives | Page files | Hibernation files | Printer spooler files | Configuration files | Documents | Spreadsheets | Journal entries | Diary entries | Calendar entries | Historical artifacts associated with Internet activity (bookmarks, favorites, cookies, browser extensions, html code, java code, etc.) | Backup data | Synchronized data | Communications and correspondence data (e.g., chat and instant messaging logs, email, PST files, attachments, web postings, etc.) | Screen names | Activity associated with file sharing networks (e.g., peer-to-peer file exchange logs) | Financial records | Multimedia files (movies, digital photographs, graphic image files, streaming data, flash, PDF files, PowerPoint presentations, blog entries, wikis , etc.) | Closed-circuit television (CCTV) recordings | Postage tracking numbers | Database entries | International Mobile Equipment Identity (IMEI) | International Mobile Subscriber Identity (IMSI) | Location data in phone registers | Contact lists | Call logs | Short Message Service (SMS) | Multimedia Message Service (MMS) | Notes | Memorandums | Voice mail | GPS coordinates and geo-tags | Credit card numbers | Application data | Unique equipment and subscriber numbers | Office 365 | Malware | Print, scan, and fax jobs | Physical access registers for buildings and facilities (e.g., radio frequency identification logs)
Solid State Drives (SSD)	
Virtual Machines	
Flash Storage	
Optical Discs	
Magnetic Tape Digital Storage	
Floppy Discs and Legacy Media	
Random Access Memory (RAM)	
Chipsets	
Network Devices	
Mobile Devices	
SIM Cards	
Tablets	
Digital Cameras	
Multifunction Devices	
Security Systems	
Cloud Computing Environments	
Datacenters	
Cloud Storage	
Gaming Consoles	
Online Gaming Platforms	
Social Media Platforms	
Private Branch Exchange (PBX)	

Technological innovation and trends emerging in both commercial and consumer markets drive digital forensics investigations. This constant state of flux creates investigatory and analytical challenges such that analysts must adapt to distinctive variations

in the form and source of ESI. Issues associated with 'big data' are a particular concern due to the prevalence of large and complex data sets (Caltagirone, 2015). The scope of evidence located at crime scenes is now vast and encompasses all manner of mobile devices, electronic storage mediums, and computer networking peripherals (Ritter, 2006). Many consumer devices have evolved into mobile data containers, and practically every category of crime can involve electronic evidence in some form or another (Bennett, 2012). As such, the quintessential 'smoking gun' is increasingly viewed as the quintessential 'needle in a haystack'. In reality, digital forensics investigations are a protracted process and the goal "is not pure knowledge but practical supposition" (Kelly & Wearne, 1998, p. 18). The investigative challenge is one of locating, identifying, comparing, and interpreting diverse sources of potential evidence (Mora & Kloet, 2010; PMSEIC Working Group on Science, Crime Prevention and Law Enforcement, 2000). Digital forensics employs a blend of investigative and technical methodologies to interpret findings. This approach combines scientific knowledge with practical expertise derived from repeated casework. Although forensic analysis can uncover the 'smoking gun' which makes or breaks a case (Saferstein, 1987), more often it adds value by providing intelligence to establish facts of a corroborative nature (Akin, 2011; Shavers, 2013).

As communities worldwide continue to embrace technology, digital traces associated with cyber crime offending have also become more pervasive. Both consumer and commercial devices store a wealth of user data that is increasingly integrated with web mail accounts, cloud-based services, social networking platforms, and synchronized desktop applications. This data can contain detailed sequences of events indicative of criminal intent, interrelationships between organized networks of offenders, and the whereabouts of suspects during criminal activity (see *Table 5*). However, the capacity of investigators to retrieve and forensically acquire this information is increasingly complex due to the vast range of devices, and the absence of comprehensive and affordable tools to get the job done (e.g., *United State v. Bennett*, 2004) (Bennett, 2011; Mislan, 2010).

Mary's Case: Forensic Outcomes and Warrant Activity

Forensic analysis of the email and SMS messages at the e-Crime Lab supports Lyon's initial findings. Detailed examination of metadata associated with the digital photographs also reveals embedded 'geo-tags'. Lyon plots the GPS coordinates on a map and presents the information to Mary. Mary identifies the locality as consistent with the address of Paul, her former boyfriend. Lyon takes a statement from Mary and applies to the court for search and seizure warrants targeting Paul's residence. The Magistrate grants the warrants and Lyon executes them the following day. Police search Paul's house but are unable to find the item of Mary's clothing depicted among the digital photographs. The encryption implemented on Paul's Blackberry device hinders attempts by forensic personnel to access the data. Paul refuses to provide the passphrase to decrypt the contents of his phone and telephones a lawyer who recommends that he not make any formal statement. Forensic analysis of Paul's computer exposes a quantity of child exploitation material (CEM) and digital photographs, which resemble those sent to Mary. Lyon arrests Paul and police seize his computer and Blackberry. Lyon escorts Paul to the local police station where Paul's lawyer meets them. Lyon commences a Record of Interview during which Paul makes no comment to the questions put to him. Lyon charges Paul with stalking and informs him that he may also be charged with possession of child pornography.

4. Impediments to Evidence Discovery and Analysis

4.1. Resourcing and Liability

It is estimated that by 2016 the average household will have 3.3 terabytes of data stored across various devices (Lee, 2014). The quantity of raw data collected during investigations places great pressure on investigators and analysts to deliver reliable results in very short timeframes (Holt & Blevins, 2008). A steady increase in the density of flash and magnetic disk storage explains why many law enforcement agencies are burdened with extensive backlogs of devices awaiting analysis. It is common for investigations into cyber crime offending to become 'fishing expeditions' without proper regard for the probative value of seized devices. Due to the practical limits of investigative and analytical labor and shifting case priorities, it is regularly infeasible to scrutinize all data housed across the full gamut of electronic devices discovered at crime scenes (Gill & Phythian, 2012). As is evident in Mary's Case, a shared problem among law enforcement agencies globally concerns delays in processing devices for forensic analysis. These analytical bottlenecks are exacerbated by the absence of triage strategies and the inadequacy of budgets for procurement, staffing, and training (Raymond, 2006). The problem is further compounded by a general misperception among senior management bureaucrats that digital forensics can achieve more with fewer personnel due to increases in computer processing power and automation.

When police attend business premises during warrant activity, and suspended or interrupt networked computing services to collect ESI, there may be legal ramifications (Middleton, 2002). Disrupting or hampering business operations can expose investigating authorities to protracted litigation and liability. Court ordered damages for obstructing moneymaking activities of major corporations could be very costly, thereby discouraging police investigations within commercial environments (e.g., *Jackson Games, Inc. v Secret Service*, 1993; *Katz v United States*, 1967; & *Berger v New York*, 1967). When police discover running devices at warrant premises they face a legal and technical conundrum. For many years, it was considered best practice among law enforcement agencies to simply 'pull the plug' and remove the power source from running devices. Nowadays, changes in hardware and software dependencies, the prevalence of consumer security, and complexities of networking architecture have necessitated a more considered approach by first responders.

Live forensics is "the means and technique of obtaining artifacts of evidential value from a machine that is running at the time of analysis" (Biggs & Vidalis, 2009). Volatile data subsisting in RAM and networking peripherals must be captured live to ensure that information is preserved (Hay, Nance& Bishop, 2009). Full disk encryption and remote connections to computing resources may also call for live forensics procedures to acquire information. However, during legal proceedings the integrity of electronic evidence may be called into question if the police are unable to explain the consequences of investigative activities performed on live systems. Ultimately, any live procedure performed on a running device creates changes to the system state. Therefore, it may be impossible to replicate the live system state to verify and validate findings, once power is removed (Carrier, 2006). It is for this reason that any activity, which changes data on a system, is discouraged. This information typically constitutes the original evidence and any modification to file metadata is akin to contaminating a crime scene (Shipley & Reeve,

2006). Nevertheless, liberties may be taken provided actions can be sufficiently explained and justified before a court of law.

Table 6. Cloud Delivery Models

Delivery Model	Description
Platform as a service (PaaS)	Cloud users install and run their own software on computing platforms (i.e., operating systems) that are maintained and managed by providers.
Infrastructure as a service (IaaS)	Cloud users lease physical and virtual computing resources (i.e., storage, computer processing power, security infrastructure) that are maintained and managed by providers.
Software as a service (SaaS)	Cloud users access and control software applications (i.e., antivirus, email servers, backup, databases, Voice over Internet Protocol) that are maintained and managed by providers.
Network as a service (NaaS)	Cloud users access networking infrastructure and network/transport connectivity services (i.e., domain controllers, custom routing, multicast protocols, bandwidth, clustering, load balancing) that are maintained and managed by providers.

Table 7. Cloud Deployment Models

Deployment Model	Description
Private cloud (internal or external)	For the sole use of an organization or user and hosted and/or managed internally or externally (i.e., enterprise owned or third party leased).
Community cloud (internal or external)	Shared infrastructure between organizations or users with common interests or concerns (e.g., academic, government, commercial, etc.) and hosted and/or managed internally or externally.
Public cloud (external)	Offered to the public free or on a pay-per-use basis and usually hosted within a multi-tenanted, large-scale infrastructure.
Hybrid cloud	Composed of two or more cloud models (i.e., private, public, community) that, whilst discrete, are configured to work together (i.e., interoperate).

4.2. Cloud Computing and Data Mapping

Personal, public and private domains are increasingly interconnected through networked infrastructure, ranging from a small number of devices connected in close proximity to literally thousands of devices linked through virtual private networks that span geographical and jurisdictional boundaries (Smith, 2004; Zatyko & Bay, 2011). The popularity of cloud computing has amplified cross-border investigative and privacy issues because domestic laws are innately local and the cloud is intrinsically global. Inside their data centers, cloud service providers (CSPs) offer access to powerful computing and networking infrastructure (Grace & Mell, 2011). Resources are delivered to users as a service that is accessed remotely over a network. The service offerings are distinguished according to functionality and delivery model (see *Table 6*). Cloud computing is a force multiplier and the expanding consumer base globally offers cyber criminals both a centralized pool of victims as well as new avenues to exploit digital resources and evade detection (Mills, 2012). Cloud services may become the target of criminal activity (e.g., unauthorized access, system sabotage, data theft, spying/stalking, etc.). In the same vein, Cloud services may also be leveraged as a means of committing criminal activity (e.g.,

drop point for exfiltrated data, vehicle for dissemination of child abuse material, platform for committing fraud and other illicit activity, watering hole for malware distribution, resource for Distributed Denial of Service Attack reflection and amplification, etc.).

Investigators regularly encounter devices connected to cloud services during warrant activity including remote desktop sessions, remote services connected to mobile devices, active Virtual Private Network (VPN) connections, and connectivity to web mail and social networking platforms. Due to automated cloud backup and synchronization among consumer devices, data is often replicated across various cloud-computing environments. This information can provide vital clues about victimization, how an offender committed a crime, and evidence of prior acts demonstrating a course of conduct. Data interception procedures employed by police agencies may facilitate access to data stored and transmitted via cloud services. However, where CSPs have operations that span multiple countries, data for individual cloud users may be geographically dispersed and potentially pooled with data from other users (i.e., multi-tenancy), depending on the cloud deployment model implemented (see *Table* 7). This significantly hinders crime scene investigation and event reconstruction. Maintaining evidence continuity can be complex as both stored and transmitted data may be retrieved from disparate points of origin within cloud computing infrastructures (i.e., trans-border data-flows, distributed file systems, data backup and replication/synchronization, etc.) which affects the legal provisions governing data access and disclosure.

Public cloud deployment within multi-tenanted infrastructure can present a minefield of privacy and technical issues for investigators (Barrett & Kippler, 2010; Huber, Mulazzani, Leithner, et al., 2011; Taylor, Haggerty, Gresty & Lamb, 2011; Subashini & Kavitha, 2011). Problems arise when the data forming the target of an investigation is stored on a physical device that is shared with other cloud users. Due to potential impact on third parties, this prohibits seizing or physically imaging the device (Cloud Security Alliance, 2010). Many digital forensics tools are also unsuited to parsing data from cloud computing environments (National Institute of Standards and Technology, 2011; Reilly, Wren & Berry, 2011). As such, police usually require the assistance of system administrators at data centers to facilitate access, retrieval, and logical acquisition of data. This interface is critical as the high standard placed on admissibility of evidence demands that investigators are able to attest that the processes used to parse and collect ESI functioned properly and did not change the data (i.e., data integrity, chain-of-custody, and verification). Data replication and use of distributed file systems by data centers for load balancing can also create issues related to data mapping as information sought by police can be dispersed across national borders. The difficulty for investigating authorities lies in mapping the location where the data is hosted, tracing the geographic trajectory through which the data flows, and establishing the laws governing data treatment within those jurisdictions (Taylor, Haggerty, Gresty & Lamb, 2011). Ultimately, many current best practice guidelines for handling electronic evidence are manifestly inadequate for undertaking investigations within the cloud.

4.3. Internet-Based and Satellite Telecommunications

When the telecommunications industry introduced digital, switch-based telecommunications services in the 1990s, the capacity of investigating authorities to intercept voice communications was significantly impaired. In the US, Congress enacted the *Communications Assistance for Law Enforcement Act* (1994) (CALEA) to overcome this

problem, requiring carriers to be able "to isolate and deliver particular communications, to the exclusion of other communications, and to be able to deliver information regarding the origination and termination of the communication" (Caproni, 2011). This is commonly referred to as dialing and signaling information or pen register information.

Before there were smart phones with Internet-based modes of communication, most digital telecommunications passed through fixed-line switches or mobile communication towers. These centralized routing configurations provided investigating authorities with a reliable source of evidence and intelligence due to the retention of subscriber and traffic data by carriers. Faculties-based storage and localized transmissions of telecommunications data through carriers also encouraged surveillance and interception activities as court orders could be sought and served with relative ease. Over time, the reach of instruments such as CALEA and RIPA expanded to include Voice over Internet Protocol (VoIP) and facilities-based broadband Internet access modalities which are entirely interconnected with the public switched telephone network.

Amendments to the *Foreign Intelligence Surveillance Act* (1978) and Title III of the *Omnibus Crime Control and Safe Streets Act* (1968) empower authorities in the US to conduct court-ordered electronic surveillance of content data transmitted via Internet-based communications. Local companies and foreign firms with business operations extending into the US must be able to comply if served with a wiretap order. This includes encrypted email services (e.g., Hushmail), social networking sites (e.g., Facebook, Instagram, LinkedIn, etc.), and providers of voice, video conferencing, instant messaging and file sharing software (e.g., Skype, WhatsApp, QQ, Viber, WeChat, Black Berry Messenger, etc.). Compliance here extends to making changes to the architecture of their services to facilitate surveillance and interception activities of investigating authorities. For example, Title III specifies that a "service provider, landlord…or other person shall furnish…forthwith all…technical assistance necessary to accomplish the interception." Authorities can also compel service providers to disclose the cryptographic keys used to secure data transmitted via their platforms. However, these legal instruments are focused primarily on telecommunications carriers that deliver mobile telephone services and traditional telephony, and do not cover popular and emerging Internet-based communications services, in a legal or technical capacity.

The advent of direct peer-to-peer networks, which can transmit communications via fixed broadband Internet connections and wireless access points, has posed a significant challenge for investigating authorities. Surveillance is much more difficult to accomplish because pure peer-to-peer networks do not have a centralized server through which packets of data are routed. Interception also becomes problematic where communications protocols leverage encryption for privacy, such as Secure Real-time Transfer Protocol (SRTP) (Forte, 2006; Schjølberg &Ghernaouti-Hélie, 2011). Law enforcement and national security agencies have lobbied "that their ability to wiretap criminal and terrorism suspects is going dark as people increasingly communicate online instead of by telephone" (Savage, 2010). This is due in part to the disbursed and private architecture of some peer-to-peer networks, including decentralized implementations of VoIP. According to the FBI, "the law hasn't kept pace with technology, and…both real-time communication and stored data are increasingly encrypted" (Comey, 2014).

> As the gap between authority and capability widens, the government is increasingly unable to collect valuable evidence in cases ranging from child exploitation and pornography to organized crime and drug trafficking to terrorism and espionage - evidence that a court has authorized the government to collect…As we discuss the Going Dark problem today, we are not focusing on access to stored data. Rather, we are focusing on the interception of electronic communications and related data in real or near-real time. Without the ability to collect these communications in real or near-real time, investigators will remain several steps behind and left unable to act quickly to disrupt threats to public safety or gather key evidence that will allow us to dismantle criminal networks (Caproni, 2011).

The mobility and secrecy afforded by encoded satellite telecommunications systems has made this technology popular among organized criminal groups (Goodman, 2011; Shelley, 2003). Although the GMR-1 and GMR-2 ciphers on common satphones have been broken (Small World News, 2012), there are still limited technical and legal avenues that most domestic policing agencies may pursue to access or intercept encoded satellite communications which move across borders. As is apparent in Mary's case, this technology challenges investigators in much the same way that broadband telephony does. Some satellite communications providers enable users to configure their service so that subscriber and content data is stored within a jurisdiction of their choosing (Di Gregory, 2000). As such, stored data becomes subject to the laws of the country where the satellite-based subscription service is located, often-placing evidence beyond the reach of law enforcement, depending on diplomatic relations between the county hosting the data and the country requesting access.

Undoubtedly, both broadband and satellite telephony have profoundly impacted the capacity of investigating authorities to access data and intercept communications. As governments pass new legislation to increase the visibility and audibility of electronic communications, the cat and mouse game between 'pursuers' and 'evaders' will intensify. Ultimately, strong encryption technology is widespread and rapidly becoming immune to unilateral or even multilateral control by nation-states. Decentralized open source secure communications platforms are emerging and gaining popularity with users (e.g. Tails, Jitsi, Freepto, etc.). These tools integrate secure instant messaging, voice, and video conferencing clients without need for signaling, public key infrastructure (PKI), or centralized servers. Off-the-Record Messaging (OTR) over Extensible Messaging Presence Protocol (XMPP) can be configured for secure instant messaging, and the Zimmerman Real-time Transport Protocol (ZRTP) may be implemented for private voice and video conferencing when transmitting over Session Initiation Protocol (SIP). However, the effectiveness of these tools and protocols is impacted by the trustworthiness of each end point. If one or both parties to a communication are infiltrated and the base operating system is compromised, transmissions may be intercepted with ease. Effective use of these protocols and systems also requires some mindfulness and technical engagement by the user, thereby posing a potential security problem in itself.

4.4. Anonymization

Email data is often a vital source of evidence for police investigations. Header information within email threads can assist police in identifying the origin of a communication and may even pinpoint to the physical location of a suspect. Message content and email attachments can also disclose personal particulars about offenders and co-conspirators, including financial transactions and direct evidence related to criminal activity, as well as detailed records of communications between perpetrators and victims.

Criminals that employ sophisticated methods of offending are well aware of vulnerabilities associated with normal email transmissions. Instead, they will use secure web-based email services, remailers, and other anonymizing methods to communicate discretely. Anonymization techniques are specially crafted to conceal a user's identity when navigating the Internet or sending communications (Morris, 2004). Anonymizing remailers are actually intermediary mail servers that function as a gate between the sender of an email and the recipient. When email passes through the remailer service, identifying information is stripped from the email header. Message content, including attachments, can then be anonymously forwarded to the recipient. As is evident in Mary's Case, identifying the origin of email transmitted via remailers is problematic as these services may not maintain lists of actual senders, in some jurisdictions (Clough, 2011; Denning & Baugh, 1999; Wettering, 2001). Like the enhanced security features available on peer-to-peer network clients, cryptography also poses potential stumbling blocks for investigating authorities (e.g., Dark Mail Alliance, Open Whisper Systems, etc.). The non-proprietary version of the Pretty Good Privacy software (OpenPGP) can be leveraged with ease to send and receive signed encrypted email messages.

When email is stored remotely, investigators will be lucky to recover web mail fragments during static analysis of Internet history on computers and devices. 'Dead-dropping' is a technique that exploits web mail services to enable covert communications. In practice, suspects share account credentials and communicate in secret through unsent messages that are saved within web mail accounts based in jurisdictions beyond the reach of investigating authorities. This method of exchange allows information to pass between parties to a communication, without risk of interception that occurs when email messages are transmitted over the Internet. Criminals have been shown to access these 'virtual drop points' through public access terminals and Internet hotspots in an attempt to evade detection (Adams, 2003; Caulfield & Buttler, 2003). This strategy can create difficulties for police when attempting to identify offenders based on IP tracing alone.

Cyber crime offenders also exploit proxy servers to conceal online activity (Spence-Diehl, 2003). Proxy services enable users to establish a connection to a network via an intermediary server. Common proxy servers can be configured for access control, caching services, and enhanced information security (Brown, 2015). Anonymous proxies also permit users to subscribe with cash or Bitcoin payments to conceal or misrepresent their identity during the registration process. Once configured, an encrypted 'multi-hop' proxy service can be leveraged to hide an IP address, impersonate another IP address, or redirect traffic to obscure points of origin across the network (Li, Erdin, Güneş et al., 2011). Mary's Case illustrates how use of proxy services to reroute network traffic through foreign jurisdictions can manifestly increase the difficulty of attributing activity to a suspect. In 2015, the Independent Reviewer of Terrorism Legislation in the UK

contended that a complete overhaul of the law is needed to address challenges created by advancements in technology.

> Modern communications networks can be used by the unscrupulous for purposes ranging from cyber-attack, terrorism and espionage to fraud, kidnap and child sexual exploitation. A successful response to these threats depends on entrusting public bodies with the powers they need to identify and follow suspects in a borderless online world. But trust requires verification. Each intrusive power must be shown to be necessary, clearly spelled out in law, limited in accordance with international human rights standards and subject to demanding and visible safeguards. The current law is fragmented, obscure, under constant challenge and variable in the protections that it affords the innocent. It is time for a clean slate (Anderson, 2015).

4.5. Obfuscation and Encryption

When executing search and seizure warrants it can be very difficult for police to physically locate devices at crime scenes and other premises. Flash storage is often integrated within common household appliances and personal items such as toys, pens, sunglasses, watches, jewelry, and luggage tags (Young, 2009). Micro Secure Digital (SD) cards, mobile SSDs, and wireless storage devices can be concealed within wall cavities, under tiles, and inside ceiling and floor spaces. Even if investigators are able to find hidden devices, the content of data stored on those devices may have been encoded. Steganography is an 'information-smuggling' technique that disguises information inside the code of ordinary files, such as graphic images, documents and audio recordings (Graham, Howard & Olson, 2011). Media files are ideal hosts for steganography as they are quite large and will not immediately arouse suspicion during analysis (Li, He, Huang, et al., 2011; Shelly, 2004). Investigators may be able to detect the use of steganography by applying 'steganalysis' to compare the signature of a suspect file against a known original to identify inconsistencies. However, even steganalysis may yield little value where steganography has been combined with cryptography. Network steganography, in particular, is very difficult to detect due to surreptitious manipulation of lost, corrupt, hidden or unused data fields within network traffic. A common technique is to hide 'steganograms' within VoIP transmissions during video or audio conferencing. During an ordinary VoIP call, packets of data may be silently transferred between participants. Afterwards, these collected datagrams can be reconstituted as meaningful data (Lubacz, Mazurczyk & Szczypiorski, 2010). The use of steganography to conceal and deliver malicious code is also an evolving technique leveraged by malware authors to evade network and host-based detection mechanisms (Dell SecureWorks, 2015).

It is common for offenders to infiltrate private networks to leverage 'hijacked' resources for cover or camouflage whilst engaging in crime. Offenders also rely on public access points to enhance anonymity, mobility, and avoid surveillance. Domains can also be registered with holding companies, which function to cloak the domain user, and blocks of IP addresses can be leased and subleased. Consequently, attribution becomes very complex for investigating authorities as the entity registered for a particular domain or IP address may not be the entity in control of that resource when the criminal activity occurred (Brown, 2015). Widespread use of Classless Inter-Domain Routing (CIDR), Dynamic Host Configuration Protocol (DHCP), and Serial Line Internet Protocol (SLIP) has also convoluted the process of identifying end points on the Internet. Network traffic

can be effectively concealed using dedicated network protocols such as SOCKet Secure (SOCKS), Secure Shell (SSH), Secure Sockets Layer (SSL), Point-to-Point Protocol (PPP), Remote Management and Control Protocol (RMCP), Secure/Multipurpose Internet Mail Extensions (S/MIME), Direct Internet Message Encapsulation (DIME), Address Resolution Protocol (ARP), Internet Protocol Security (IPSec), and VPN tunneling (Brown, 2015).

Evidently, strong encryption poses an immense challenge for investigations into cyber crime offending, and has done so for many years (Ashford, 2015; Fisher, 2015; Cordero, & Zwillinger, 2015; Kaspersen, 1995). Intelligence and law enforcement officials have become more vocal in their cautioning that growing use of encryption seriously hinders investigations (Nakashima & Gellman, 2015). Intercepting network traffic and seizing devices is often a fruitless exercise when a suspect has implemented robust encryption on disks and handsets for data at rest, in conjunction with encrypted channels of communication for data in transit. Whilst some suspects may be inclined to disclose passphrases to police when asked, this is highly dependent upon the criminal offending concerned. For crimes associated with child abuse material, suspects are usually uncooperative due to the legal consequences of their crimes (i.e., incarceration, registration as a sex offender, public shame and humiliation, etc.). The element of surprise can assist police greatly when executing warrants, particularly if offenders are apprehended whilst using their devices and remote connections are active, and stored data is in a decrypted state (McAllister, 2015). Some jurisdictions even empower police to obtain court orders compelling suspects to divulge decryption keys. Failure to comply with such a court order usually carries a term of imprisonment (e.g., Part III of the *Regulation of Investigatory Powers Act*, 2000, UK; Schedule 2 of the *Cyber crime Act*, 2001, Australia, etc.).

During cyber crime investigations police often succeeded in detecting technology used in the commission of a crime but are unable to place an offender 'behind the keyboard' due to full drive encryption or where there is more than one user of the suspect device. In such circumstances, surveillance by way of keystroke monitor in combination with hidden camera may reveal passphrases and identify an offender (Wade, 2011). However, police powers in some jurisdictions do not extend use of invasive surveillance for cyber crime offending and many law enforcement agencies lack the technical means of circumventing strong encryption. Small-encrypted containers concealed amongst large volumes of data can be difficult to identify. Moreover, suspects often conveniently forget passphrases required to decrypt data, even when disclosure is ordered by a court of law. Some tools also incorporate 'deniable encryption technology', which enables users to create multiple containers with discrete passphrases so that users can maintain the secrecy of a hidden volume when disclosure is enforced. Whilst there are techniques for revealing the existence of 'hidden encrypted volumes' based on entropy testing, code cracking is currently a daunting challenge for policing agencies in particular.

In response to increasing pressure from consumers and the international community (Office of the United Nations High Commissioner for Human Rights, 2015), multinational corporations such as Apple and Google are integrating next-generation encryption technology on smart phones that is secure-by-default (Apple, 2015; Editorial Board, 2014; Wilber, 2015). This poses a major obstacle for law enforcement as "the companies themselves won't be able to unlock phones, laptops, and tablets to reveal photos, documents, e-mail, and recordings stored within" (Comey, 2014). There are

polarized views among participants engaged in this heated debate (Timberg, 2014). Little common ground exists between those advocating for enhanced consumer security and officials who are forecasting an escalation in unsolved violent crime, increases in terrorist attacks, and anguish for victims who may never see justice (Pelroth, 2015). Various compromises have been suggested, including embedding backdoors within encryption technologies or retaining decryption keys in escrow to facilitate access for investigators (Hall, 2015; Schaul, 2015; Swire & Ahmad, 2012). Whilst domestic laws can require companies operating within a jurisdiction to give authorities access to data housed on their local servers, legislation cannot compel foreign firms that do not possess the keys to consumer devices to somehow create them. The extent of hostility towards encryption controls is best illustrated in the following quotation from a founding member of the Electronic Frontier Foundation: "You can have my encryption algorithm . . . when you pry my cold dead fingers from its private key" (Barlow, 1992, p. 29). Some contend that the sun is setting on the golden age of surveillance, yet the dawn of quantum computing will likely ensure that investigating authorities are not left in the dark for too long. Due to substantial increases in processing power afforded by quantum computing, the potential exists to vastly improve brute force attacks against encryption algorithms (Anonymous, 2015; Poeter, 2012; Simonite, 2014; Thompson, 2014; Wadhwa, 2015).

Mary's Case: Modus Operandi

Lyon follows up with up with the e-Crime Lab to see if they have been able to defeat the encryption on Paul's phone. The Lab reports that they have not been able to circumvent security on the Blackberry, and have not identified how the CEM was downloaded to Paul's computer, or the electronic means used to stalk Mary. However, the Lab reports that the digital photographs discovered on Paul's computer match those sent to Mary. Lyon prepares a short-form brief of evidence for delivery to the Office of Public Prosecutions (OPP). A few weeks later, James Keller, a prosecutor with the OPP, arranges for a meeting with Lyons. Keller informs Lyon that he has received correspondence from Paul's lawyer indicating that Paul intends to contest the charges. Keller predicts that, in the absence of corroborative evidence, the defense will argue that Paul did not knowingly possess the CEM. Lyon speculates that Paul used his Blackberry to instigate the cyber-stalking and to download the CEM. Keller recommends that Lyon apply to the court for an order compelling Paul to provide the decryption passphrase for his Blackberry.

5. Legal Process

5.1. Rules of Evidence

Evidence can be conceived as a branch of the law that consists of rules and procedures governing the proof of a particular set of facts in issue. Matters of evidence are concerned with determining which facts may or may not be proved, the type of evidence that may be given in support of such facts, and by whom and in what manner the evidence may be proved. In a criminal trial, the fundamental question in issue is the guilt or innocence of the accused. Any material used in determining this issue, which is allowed under the law of a particular jurisdiction, is evidence and may consist of facts, testimony, documents, and physical exhibits which may be admitted to prove or disprove the facts under inquiry. In common law countries, evidence "is the means by which the prosecuting authority

seeks to establish the guilt of the accused party, and also the means by which the defense teams seek to establish their client's innocence" (Jones, 2006, p. 273).

Information does not assume the character of evidence until the court says it does and limits exist on what information can be put before the court. Rules of evidence function like a gate through which information must pass prior to being formally admitted as evidence. If the information passes through the gate, it may only then be properly called evidence. If it does not pass, the information is excluded and is not available to the fact-finder for consideration. Threshold questions will often arise as to whether an item of evidence meets the test of admissibility under the relevant rules of evidence governing an inquiry. The question of admissibility is a matter of law and evidence is generally admissible where it is relevant to a fact in issue, its probative value outweighs its prejudicial effect, and the material is not excluded by a rule of evidence. Once admitted, evidence may be used by the court for any legitimate purpose. Where the evidence is capable of supporting the prosecution and defense cases, the fact-finder must decide which view prevails, if any.

As a general principle, courts are entitled to the best evidence that is available. Best evidence is that which is regarded by the law as affording greatest certainty of the fact in question. When the best evidence rule is applied, a copy will not be admissible unless it can be demonstrated that the original is unavailable due to destruction or other circumstances, and that secondary evidence, such as copies, notes or other testimony, is the best that the circumstances of the case will allow. Printouts of information from computers or other devices may not be regarded as original given the same information in digital form is comprised of machine-readable data (i.e., binary code). These strings of '1s' and '0s' must be read by a computer program to define what should be done with the coded data, which is intended to generate human-perceivable information. The issue here relates to whether the human-perceivable form of the digital information as presented to a court (e.g., a printed document) is an accurate representation of that information in its original binary form (Chaikin, 2006). However, the best evidence rule usually does not operate to exclude printed information, provided the printout accurately reflects the data (e.g., *Doe v United States*, 1992; *Laughner v State*, 2002).

Hearsay evidence is a form of testimonial evidence and is the most complex of the exclusionary rules of evidence in common law jurisdictions. Authorities agree that hearsay encompasses instances where a witness retells the court about a statement made by another person out-of-court, and where the substance of that statement is being used to prove the truth of the facts in issue. This form of evidence may be declared inadmissible when it is introduced to prove the truth of what was asserted in that out-of-court statement (U.S. Department of Justice, 'Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors', 2007). In situations where the statement is not offered to prove the truth of the statement (i.e., the truthfulness of what was said), but rather merely the fact that the statement was made, it is not considered hearsay and may be admissible. Under the hearsay rule, the expression 'statement' applies equally to both verbal and written statements, and in some cases the conduct of a person may also be considered as a statement. The reason for the general inadmissibility of hearsay is that such statements are potentially unreliable with little or no assurances or means of checking their actual reliability (e.g., *Ohio v Roberts*, 1980). In many common law jurisdictions the courts have accepted that business records maintained electronically are admissible into evidence as an

exception to the hearsay rule if it can be demonstrated that the document is reliable (e.g., *Harris v Smith*, 1967; *Hughes v United States*, 1992; *United States v Catabran*, 1988; *United States v Cestnik*, 1994).

Due to issues of proximity and remoteness, the identification of cyber crime offending will often rely on circumstantial evidence to establish that a particular suspect was in control of a device when an offence occurred. Circumstantial evidence establishes facts by inference from other proven facts. As such, circumstantial evidence is indirect evidence relating to matters that in isolation do not amount to direct evidence of any fact in issue but from which facts in issue, or matters relevant to facts in issue, may reasonably be inferred. Circumstantial evidence can be extremely valuable in verifying authorship and authenticity of information (e.g., metadata, witness statements, background checks, timeline analysis, Internet browsing history, activity on social networking websites, data retained by service providers, etc.). When the prosecution seeks to rely on circumstantial evidence to establish guilt, all reasonable hypotheses consistent with the innocence of a defendant must be excluded. In other words, the tribunal of fact (i.e., judge or jury) must be satisfied beyond reasonable doubt that all elements of the offence are proved. Accordingly, the only reasonable inference to be drawn from the evidence in its entirety, and not by considering individual items of evidence in isolation that cannot support the inference sought, is that the defendant is guilty as charged (e.g., *PP v Neo Koon Seng*, 2008; *United States v Siddiqui*, 2000; *United States v Simpson*, 1998; *United States v Tank*, 2000).

5.2. Computer-Generated and Computer-Stored Information

Some jurisdictions differentiate between computer-generated records created by a computer as an automatic function of the operating system or program, and computer-stored records such as those created by the computer user through manual input (e.g., *People v Holowko*, 1985). The theoretical difference between these sources of ESI pivots on whether a human or machine created the content (e.g., *State v Swinton*, 2004). However, this distinction lacks precision in a practical sense (Teppler, 2009). Regardless of who or what created the data, it is usually the metadata that is critical for investigators and prosecutors when seeking to substantiate elements of an offence (Buchholz & Tjaden, 2007; Koen & Olivier, 2008; Weil, 2002). Yet this metadata can be easily modified, overwritten or deleted, thus posing unique problems for investigators. It is not uncommon for internal clocks and time zone settings in computers, digital cameras and other mobile devices to be inaccurate. Moreover, times and dates reflected in email headers may lack consistency as messages are routed through servers located in different time zones, which themselves may be unreliable (e.g., *United States v Whitaker*, 1997). The evidentiary issue pertains to the trustworthiness of the operating system or program which generated the information, and whether that process was functioning properly (Lempert & Saltzburg, 1983). This does not necessarily affect the admissibility of the evidence, but may influence the weight given to the evidence (e.g., *United States v Catabran*, 1988).

Mary's Case: Mandatory Disclosure and Committal Hearing

Lyon obtains an order from the court under section 3LA of the Crimes Act 1914 (Cth) requiring Paul to divulge information needed to access data held in his Blackberry. The court order is served upon Paul's solicitor and Lyon receives the decryption passphrase in subsequent correspondence. Other than Mary's contact details, digital forensic analysis of the Blackberry does not reveal any evidence to support the stalking or possession charges. Detailed examination of Internet browsing history on the phone shows records consistent with an interest in gay dating websites and recreational drug use. Lyon meets again with the OPP to review the evidence. Despite the absence of evidence on the Blackberry, Keller is still confident that a prima facie case exists against Paul and therefore proceeds with a charge for possession of child pornography. The matter is listed for Committal Hearing in the Magistrates' Court. At the Hearing, the Defense Counsel enters a submission of 'no case to answer', asserting that the defendant did not have any knowledge of the CEM on his computer, that someone else placed it there, and disputing the authenticity of the digital photographs related to the stalking charge. The Magistrate struggles to understand the technical subject matter and orders that the possession and stalking charges be listed for separate trials in the County Court. Defense Counsel then applies to have the charges tried jointly.

5.3. Legal Challenges to Electronic Evidence

In 1798, Lord Kenyon declared, "it is a principle of natural justice, and of our law, that *actus non facitreum nisi mens sit rea*. The intent and the act must both concur to constitute the crime." In other words, for serious crimes in common law jurisdictions the prosecution must establish both the physical and mental elements of an offence to convict the defendant. The *physical element* or *external element* is referred to as *'actus reus*'. This represents actual activities undertaken in the furtherance of a crime. The *mental* or *fault element* is known as *'mens rea*'. This element embodies the knowledge, mindfulness or intent to carry out a crime. The determination of criminal responsibility for serious crimes usually requires that the *criminal act* and the *criminal intent*, or *fault element*, coincide (*Fowler v Padget*, 1798). It is incumbent for investigators and prosecutors to identify elements of an offence with precision in order to frame the charge with accuracy. Prosecutors, in particular, require special training to develop the level of understanding needed to present convincing cases in court. However, understaffing and competing caseloads is a problem in many criminal justice systems. Many prosecutors are unable to dedicate the time necessary for anticipating and rebutting novel arguments mounted by opposing counsel. Such arguments are often skillfully crafted to 'muddy the water' and confuse the fact-finder (Pallaras, 2011).

As discussed earlier, it can be very difficult to establish a link between electronic evidence and an offender (Akin, 2011). Typically a mix of direct and circumstantial evidence must be assembled to place a suspect 'behind a device' at a particular time and place (Davidoff & Ham, 2012; Middleton, 2002; Shavers, 2013; Zheng, Qin, Huang & Chen, 2003). Electronic evidence is usually supplemented by evidence obtained through traditional police investigations to demonstrate that a particular device was under the control of a suspect when the offending occurred. In cases where the defendant is charged with possession of illegal material, the prosecution will need to establish that the defendant had knowledge of, and therefore intended to possess, the material. Electronic evidence is often transient and rarely exists in isolation. It is a product of the computer program used to generate the information and the computer system, which directed the activity

(Noblett, Pollitt & Presley, 2000). The question of authorship is regularly raised in cyber crime investigations, from theft of intellectual property to money laundering, as well as many types of fraud (e.g., *United States v Dioguardi*, 1970; *United States v Duncan*, 1990; *United States v Liebert*, 1975; *United States v Salgado*, 2001). If an operating system or software application contains serious programming errors then the authenticity of any computer-generated records may be challenged, depending on the circumstances of the case (Schweitzer, 2003). Departures from recognized investigative and forensics best practices are also likely to be seized upon by defense counsel, many of whom are masters at sowing seeds of doubt in the courtroom.

The authenticity of ESI is often contested by raising questions of identity concerning the author of computer-stored records (Chaski, 2005); questioning whether the computer-stored and computer-generated records have been corrupted, manipulated or altered after they were created; and by challenging the reliability of the computer program which produced the records (Kerr, 2001). Defense counsel may also contest the validity of a warrant, or argue that the investigator exceeded the scope of the warrant, and seek to have evidence excluded. Where there are multiple users of a computer or device and an absence of security controls (e.g., authentication, encryption, antivirus, firewall, etc.) opposing counsel may argue that someone or something other than the defendant generated the information (Casey, 2001). This issue may also arise when parties seek to establish authorship of computer-stored information (e.g., documents, photographs, spreadsheet, etc.) or when trying to identify parties to a communication (e.g., *R v Fraser*, 2011). In the event that malware is discovered, counsel may raise the 'Trojan Horse Defense' or 'Bot Defense' (Allison, 2003; Brenner, Carrier & Henninger, 2004; Haagman & Ghavalas, 2005; U.S. Department of Justice, 'Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors', 2007). This is a legal and technical line of argument. Accordingly, the party raising the defense asserts that autonomous malicious code, or remotely controlled rogue software (i.e., RAT), present or previously resident on the host information system, caused the offence to be committed, without the knowledge of the defendant (e.g., *R v Caffrey*, 2003).

The quality of the processes used to preserve the integrity of ESI, from the moment of creation to the point that it is introduced in court, must be demonstrated by the proponent of the evidence to substantiate its reliability and trustworthiness (Rogers, 2011; Schjølberg & Ghernaouti-Hélie, 2011). The chain-of-custody process is used to verify that the proffered evidence is free from tampering or alteration (Dubord, 2008). Evidence continuity is typically a question of fact and the chain-of-custody process is the mechanism applied to maintain and document the chronological history of evidence as it moves from one place to another. The chain-of-custody rule insures that any information presented as evidence is in substantively the same state as it was when seized (e.g., *United States v. Brown*, 1973; *United States v. Grant*, 1992; *United States v. Santiago*, 1976). In the case of ESI, evidence continuity must be maintained for both the physical device housing the data, and the information stored on the device itself. The party offering the evidence must demonstrate to the fact-finder that the information retrieved from the device is a true and accurate representation of the original data encoded on the device (i.e., authenticity). It must also be demonstrated that the physical device sought to be introduced as evidence is identical to that which was initially discovered and subsequently taken into custody (Arms, 2000; Sanett, 2000).

When a party specifically puts the issue of evidence continuity before the court, numerous objections may be led (e.g., relevance, hearsay, authenticity, integrity, etc.) (Pallaras, 2011). Defense counsel may seek to show that the device is not what is purported and that the data is therefore untrustworthy. The vulnerability of digital information to manipulation has been considered by courts with emphasis on "the need to show the accuracy of the computer in the retention and retrieval of the information at issue" (*Re VeeVinhnee, Debtor American Express Travel Related Services Company, Inc v VeeVinhnee*, 2006, at 437). In the event that the chain-of-custody is incomplete, the proffered evidence may nevertheless be admitted. This is ultimately a decision for the judge who must evaluate the severity of the break in continuity and how this influences the weight accorded to the evidence by the fact-finder during proceedings (Marcella & Greenfield, 2002).

The admissibility of information, which records activities on a computer, network, or other device, may also be open to challenge when the system generating the information does not have robust security mechanisms in place (Chaikin, 2006). An absence of strong user authentication and insufficient access controls, which adhere to the 'principle of least privilege', can also be leveraged to mount legal arguments challenging the reliability of digital information. Deficient security precautions expose information systems to manipulation and this vulnerability can undermine the credibility of data in the eyes of the court. The integrity of the evidence may also be contested in the wake of a system compromise or breach. In this scenario, defense counsel may argue that it is highly probable that sources of exculpatory evidence have been destroyed during the incident, or lost as a consequence of remediation actions performed on the system after the event.

5.4. Adjudicators, Experts and the Media

The judge and jury are ultimately responsible for determining the guilt or innocence of the accused. The standard of proof for criminal trials in common law countries is 'beyond reasonable doubt'. This means the judge or jury must be certain about the guilt of the accused. The judge functions as the arbitrator and referee in relation to clarifying the law, and typically only intervenes on issues of procedural fairness. In this way, the court's role is largely confined to overseeing the introduction of evidence to ensure that it complies with rules governing admissibility and then weighing the magnitude of that evidence to establish whether any reasonable doubt exists. However, a lack of enthusiasm by many judges to give weight to intangible sources of evidence has led to reluctance by prosecutors to use electronic evidence to support a case. There is also an inclination to rely on what lawyers already understand concerning conventional sources of evidence.

The reasons underlying this aversion are difficult to ascertain but, for the most part, criminal justice systems globally have been troubled by the pervasiveness of cyber crime offending and the haste with which electronic evidence is penetrating courtrooms. Many lawyers, judges and jurors also poorly comprehend the complexity of electronic evidence. Some lawyers "admit that they mentally switch off for the forensic evidence at a trial and that barristers avoid asking detailed questions of forensic witnesses for fear of asking one question too many" (Hamer, 1992, p. 30). The resources required to support an investigation and prosecution are both costly and time consuming. When faced with increasing workload pressures, prosecutors in common law countries must decide which cases to take on. These decisions are usually based on the perceived seriousness of the

crime, adequacy of evidence, impact that the offending has upon society, and the deterrent value of a successful conviction (Grabosky, 2007). Moreover, most courtrooms are not equipped with the technology required to present electronic evidence as a live medium. These challenges explain why many cyber crime cases are dropped before ever going to trial (Akin, 2011).

As the search for the means to combat cyber crime has intensified, so have the expectations (Julian et al., 2011; Robertson, 2004; Robertson, 2012). The potential for electronic evidence to contribute toward outcomes in criminal trials is dependent upon the attitudes of non-technical stakeholders, such as the police, prosecutors, lawyers, and the judiciary. It is vital that experts, lawyers, judges and laypeople have an awareness of precisely what constitutes electronic evidence and the limits of cyber crime inquiry. An Officer of the Court has a general duty to assist the court in the administration of justice (*Gianarelli v Wraith*, 1988). Nevertheless, lawyers and experts have a tendency to present forensic evidence in a manner that "reflects a mathematical expression of probability rather than proof beyond reasonable doubt" (Flatman, 2004; Pallaras, 2011, p. 78; Warren, 2009). The manner in which the media portrays the capabilities and expediency of forensic methodologies via television, cinema, and literature, manifestly distorts expectations (Nanji, 2005; Thomas, 2006; Willing, 2008). In reality, forensic inquiry is necessarily a protracted process. Laboratory staff, investigators, prosecutors and judges all work under intense performance and resource stressors (Gilbert, 2004), making mistakes and oversights more likely (e.g., *R v Button*, 2001). Welfare issues also arise as criminal justice officers are repeatedly exposed to obscene material (Edelmann, 2010).

Expert witnesses are regularly called upon to assist the court in criminal trials (Freckelton & Selby, 2005). The ability to communicate authoritatively, maintain composure under rigorous cross-examination, and convey essential characteristics of the evidence for the judge and jury are essential qualities when delivering expert testimony (Bologna & Lindquist, 1987). In particular, experts across all disciplines of forensic science must be able to explain the techniques applied during analysis and offer clear explanation and interpretation of results (Eckert, 1980). Success here is measured on weight of scientific findings (Neufeld & Colman, 1990), acceptance of the methodology implemented to arrive at proffered conclusions, and concise delivery of testimony to give the evidence meaning for the fact-finder, without oversimplifying the scientific basis of the findings (Gold, 1992).

In a courtroom inquiry the technical material that expert witnesses report upon can confuse the fact-finder (Phillips & Bowen, 1989). Some members of the judiciary have become concerned with the quality of expert testimony and the misleading influence that it may exert upon the jury (Kirby, 2008). Glaring issues include expert bias, failure to substantiate the basis of an opinion, unnecessary use of jargon, and practitioners exceeding their scope of expertise (Freckelton, Reddy & Selby, 1991; Freckelton, Reddy & Selby, 2001). The influence of misleading testimony and difficulties distinguishing between "genuine" and "junk science" can lead to miscarriages of justice (Eckert, 1990, p. 70). In the absence of persuasive rebuttal or conflicting expert opinion, many tribunals of fact must simply accept the uncontested assertions made by 'experts' regarding the evidence (Jasanoff, 1995). Discrepancies in legal and scientific vocabulary among jurisdictions can also create problems for those seeking to comprehend scientific findings and the legal basis of decisions.

Some commentators also maintain that forensic science suffers from poor documentation and lack of transparency (Kelly & Wearne, 1998). On occasion forensic reports have been shown to overstate conclusions (Freckelton & Selby, 2005). Imprecise and improper use of language has been shown to lack reasonable scientific certainty or coherence. Unqualified findings, which are casually described as a 'match' or 'identical to' can lead to wrongful convictions (Field, Coyle, Starmer, et al., 2009). There are universal caveats within forensic disciplines that are essential for denoting degrees of certainty and limiting the amount of weight that can and cannot be credited to results obtained (Colman, 1990). These principles comprise qualifying statements such as "including but not excluding", "possible but not certain", and "compatible with but not incompatible with" (Kelly & Wearne, 1998, p. 21).

Mary's Case: Criminal Trial

At Trial, the Prosecution presents their case against Paul (the Defendant) based on possession of CEM and discovery of digital photographs on his computer which are related to the stalking matter. In particular, the Prosecutor submits that there is no reasonable explanation beyond the Defendant having intentionally saved the CEM to his computer and engaged in cyber-stalking behavior against Mary (the Victim). It is alleged that the Defendant used anonymizing techniques to hide his identity and data sanitizing software to wipe evidence of his actions from the Internet history registry in his computer. In relation to the Blackberry device, the Prosecutor contends that the Defendant deliberately delayed police from accessing his phone to ensure that any incriminating evidence was purged from the device, as an automatic function of the software on the Blackberry. A Digital Forensic Analyst from the e-Crime Unit gives testimonial evidence about various aspects of the electronic evidence in support of the prosecution's case.

During cross-examination, Defense Counsel asks the Analyst about the digital photographs. He queries whether the photographs sent to the Victim are the same as those identified on the Defendant's computer. The Analyst states that they are mathematically identical. Counsel then inquires if these photographs were produced by the Defendant's Blackberry phone. The Analyst states that metadata embedded within the photographs is indicative that they were captured on the same Blackberry device as that owned by the Defendant. Counsel then probes about the exactness of the geo-tags embedded within these photographs. The Analyst tells the court that, whilst it is difficult to be certain about the precision of the GPS coordinates, he believes accuracy to be typically within a few meters. Before the witness is dismissed, Counsel queries whether the Analyst discovered any information on the computer or phone indicating that the Defendant harbored animosity towards the Victim. The Analyst qualifies that, other than the photographs and Mary's contact details, he did not find any other information linking the Defendant to the Victim.

Defense Counsel then calls an Independent Expert in Digital Forensics from a private security firm. The Expert gives testimony that there are disparities between the time and date information associated with the digital photographs received by the Victim on her phone and those discovered by police on the Defendant's computer. The Expert also tells the court that, whilst metadata in these photographs indicates that they were indeed captured using a Blackberry device matching the model owned by the Defendant, the device software used to produce the photographs is newer, signifying that a different Blackberry device to that owned by the Defendant was used to capture the photographs. Defense counsel then asks about the CEM. The Expert states that her analysis of the file paths associated with both the CEM material and digital photographs shows that all files are located in a shared folder on the Defendant's computer. Examination of the time and date stamps indicates that

the digital photographs were saved to the computer at about the same time as the CEM. Counsel asks the Expert what this may signify. The Expert states that, in her opinion, it is possible that the Defendant's computer was accessed remotely through an Internet connection and that the CEM and digital photographs were placed in the shared folder at this time. The Expert also testifies that, due to the lack of security precautions on the Defendant's computer, unauthorized remote activity could be performed on the computer without his knowledge or input.

Defense Counsel then calls the Defendant. Counsel asks the Defendant to explain to the Court why he was hesitant to give police access to his Blackberry phone. The Defendant states that he is homosexual but at the time had not yet disclosed his sexual orientation. In particular, he was very concerned about how his family would react to the news when the content of his phone was revealed, especially given that his family are devout Catholics. Counsel then asks the Defendant about his proficiency with computer-related technology. The Defendant states that he is a user of average ability and that his former girlfriend had assisted him with purchasing and configuring his computer. Counsel then asks the Defendant if his former girlfriend is present in the Courtroom. The Defendant states that she is present and gestures towards the Victim. Counsel then inquires about his relationship to the Victim. The Defendant states that they met at university whilst he was studying Architecture and she was completing her postgraduate studies in Computer Science. He ended the relationship with her upon realizing his persuasion towards men. Counsel then probes about the nature of their 'breakup'. The Defendant states that the Victim was very emotional and had vehemently accused him of being unfaithful with one of her male friends.

At this point, the Prosecution leads various objections. The Judge vigorously pounds his gavel on the timber bench and orders that the matter be adjourned, pending further investigation.

Recommendations

The development and promotion of national, regional, and international polices related to collecting electronic evidence, including improving national, regional and international coordination between law enforcement agencies, has seen some progress in recent years. However, the vast network of international telecommunications systems which facilitate cross-border cyber crime offending demands a common universal framework that is not just regionally centered or organizationally exclusive. Ideally, this should take the form of a binding legal instrument such as a convention on cyber crime under the auspices of the United Nations. Whilst the *Budapest Convention* has been ratified by non-member states, it is nonetheless a product of a regional organization, which is based mostly on premises and conditions of CoE members. Contrastingly, a United Nations convention would be considered a joint product of its 193 member states, and arguably offer broader appeal to the international community, thereby limiting safe harbor for cyber crime offenders.

In many common law countries, there exists significant divergence between the law in action and the law in books. Legislation must give greater attention to the realities of the function performed by police and the impact that technology exerts upon investigations, forensic inquiries and prosecutions. Mandatory assistance provisions compelling third parties, particularly service providers, to cooperate with law enforcement greatly enhances efficiency. Enacting and enforcing legislation to compel cooperation by suspects also assists in neutralizing some of the impact of encryption. Provisions for expedited preservation of ESI, streamlining requests for MLA, and expansion of the 24/7 contact system would manifestly reduce blockages to the administration of criminal justice. Where there is a 'measurable risk' of evidence destruction, police must be able to perform cursory searches of devices without need to obtain a warrant.

Shifting the burden of proof to defendants for lesser crimes by increasing strict liability categories of cyber crime offending would noticeably raise conviction rates and act as a potent deterrent. Making individuals and organizations legally obliged to implement sufficient information security precautions to protect themselves would also reduce vulnerability to cyber crime (e.g., *EU Data Protection Directive* 95/46/EC, Article 17). In some jurisdictions, unauthorized access only contravenes the law when security measures on targeted devices or systems have been circumvented or 'hacked'. If a victimized user or organization has not implemented adequate security safeguards, there is a perception that the 'victim' has failed to exercise the due diligence necessary to dissuade the criminal activity. However, any model which places an onus on the victim to demonstrate implementation of effective security defenses would need to be aligned with vastly improved efforts to raise awareness about information security architectures and the 'cyber threat landscape'.

Unilateral and multilateral efforts to regulate cyber crime through national legal frameworks and international instruments alone are insufficient to deal with transnational dimensions of cyber crime offending. Increased cooperation between international policing agencies is essential for broadening awareness concerning emerging cyber crime trends and foreign mechanisms of criminal justice (Alkaabi, Mohay, McCullagh & Chantler, 2010). Leading international law enforcement organizations such as the International Police Organization (Interpol), European Police Office (Europol), Federal Bureau of Investigation (FBI), Organization for Security and Co-operation in Europe (OSCE), International Association of Chiefs of Police (IACP), National Crime Agency (NCS), Australian Federal Police (AFP), and Latin American and Caribbean Community of Police Intelligence (CLACIP) must facilitate more dialogues on trans-border cyber crime offending to support more effective collaboration between countries. Networking opportunities at international conferences can open channels for informal cooperation, which may avoid bureaucratic entanglements and delays in obtaining electronic evidence pivotal to the success of prosecutions. The *Conference of the Parties to the United Nations Convention against Transnational Organized Crime and the Protocols Thereto* is a key platform for agitating high level issues between nation-states. However, more specialized events, such as the *Underground Economy Conference* or the *Annual Forum for Incident Response and Security Teams (FIRST) Conference*, offer a trusted environment where government officials, police, academics, and representatives from the private sector can share knowledge about cyber crime, cyber security, forensic methodologies, and investigative techniques.

Local policing agencies face a serious capabilities gap. Mostly, they lack the trusted relationships with industry that is enjoyed by federal governments. Similarly, state police do not benefit from the extensive budgets for developing facilities, resources, and technical expertise that federal law enforcement agencies leverage to implement electronic surveillance. In many western democracies, an absence of strict security vetting among state law enforcement agencies makes it difficult to share existing federally developed technology and intelligence among the wider law enforcement community. An effective mechanism for transferring surveillance and intercept technologies is required to ensure opportunities to circumvent serious instances of cyber crime offending are not missed. There is also a significant disconnect between policing agencies and the communications industry. Service providers tend to lack insights into the fundamental needs of law enforcement. Likewise, policing agencies are without up-to-date information concerning

developments in communication products offered by service providers. Improved coordination of information sharing is urgently needed to ensure timely dissemination of actionable intelligence and greater harmonization of understanding through needs assessments. Industry leaders are the key to developing a more robust system of public-private partnerships to guarantee industry experts coordinate effectively with the law enforcement community when addressing legal issues, encryption, and the broader impact of technology.

Given the disinclination of many lawyers to leverage technical subject matter when building a case, it is recommended that continuing professional development courses for lawyers directly address the impact of technology upon modes of criminal offending, with a focus on fraud, corruption, and data-driven acts causing personal harm. Awareness of the digital forensics discipline and characteristics of electronic evidence should also form part of ongoing training for the judiciary. As gatekeepers, it is incumbent for judges to maintain a comprehensive understanding of the material before them. Likewise, it would be worthwhile for jurors to receive foundational training in the fundamentals of electronic evidence prior to commencement of complex trials involving ESI. To ensure adequate upskilling, police and prosecutors must receive ongoing training that keeps pace with emerging trends in technology-enabled crime. Various organizations offer training programs designed to educate law enforcement about digital investigative processes, online criminality, and the Darknet (e.g., High Technology Crime Investigation Association, SANS Institute, etc.). Law schools could also vastly improve the competency of graduates by integrating a curriculum that teaches students about the probative value of electronic evidence, and the credibility of scientific testimony and expert opinion.

The impact of globalization is compelling national criminal justice systems to grapple with trans-jurisdictional issues. Therefore, it makes sense that those responsible for dispensing justice should also become more pluralistic. Judges with extensive experience in presiding over cyber crime cases should be available to assist in the adjudication of international cases using secure videoconferencing technology. To avoid escalation of costs associated with such an initiative, it may be that judges, with the requisite experience, are able to apply to an international judicial body, such as the International Criminal Court (ICC) or the International Court of Justice (ICJ), for recognition as a subject matter expert in the adjudication of cyber crime matters. Upon specialist accreditation, the national government in the jurisdiction where the judge principally sits could pay a fixed allowance, above the normal wage paid to members of the judiciary, to allow for casework associated with international matters. Such an allowance may be nominal, provided the specialist accreditation carries a modicum of prestige.

During criminal justice proceedings in most common law jurisdictions, the prosecution must be able to demonstrate that all avenues have been explored regarding the available evidence during an inquiry. To be effective in fulfilling this obligation, prosecutors must work in close consultation with first responders and crime scene investigators to provide courts with a comprehensive and accurate overview of an inquiry. The US model is a good point of reference here as prosecutors have long played an active role in planning and undertaking investigations. They are usually best positioned to judge how much, and what kind, of evidence is required to secure a conviction. Additionally, experienced and informed prosecutors can guide investigations to ensure that legal process is followed and frivolous challenges mounted by opposing counsel are subjected to judicial scrutiny. By

playing a leading role, prosecutors contribute to the effectiveness and credibility of police investigations and shape durable cases for trial.

Pre-trial conferences are often overlooked by lawyers and experts due to time constraints and competing casework. However, these 'round-table' meetings are an essential forum for dialogues between opposing counsel, forensic analysts and other witnesses. When conducted in an open and consultative atmosphere, pre-trial conferences may facilitate identification of hitherto unforeseen technical and legal issues. Dialogues at the pre-trial stage can actually obviate the need for '*voir dire*', expedite court proceedings, and engender deeper understanding regarding the more technical aspects of the evidence.

The development of standard operating procedures for investigating authorities that accord with industry best practices would certainly offer less scope for lawyers to challenge forensic methodologies and investigative techniques. The enactment of clear and transparent legislation would likewise reduce scope for technical objections to the admissibility of electronic evidence (Allen, 2005). Inportantly, the identification of policies to enhance the trustworthiness of expert testimony may assist in shepherding digital forensics methodologies into courtrooms. Ultimately, this will ensure that jurisprudential safeguards are adequately developed to validate the reliability and admissibility of electronic evidence. Governments and private sector entities need to pool their resources to educate workers within criminal justice systems concerning the legal and technical underpinnings of cyber crime offending. Clearly, both the public and private sectors have a shared interest in raising levels of awareness, improving baselines of understanding, and hardening information security postures (Ponemon Institute, 2015; Reuters, 2015; Sanger & Davis, 2015).

Given dramatic misrepresentations of digital forensics processes in the media there exists an urgent need for improved cognizance about what investigators and prosecutors can and cannot achieve in relation to countering cyber crime and convicting offenders. To prevent 'staff burnout', screening policies should be employed to avoid wasteful expenditure of resources on non-critical or immaterial cyber crime cases. Innovative use of technical volunteers can also greatly assist under-resourced police units struggling with backlogs of cases awaiting forensic analysis. For example, police in Kent County, Michigan, have used volunteers deputized by the sheriff to assist police with recovery and investigation of information stored within electronic devices (Rosendale, 2012). Despite having little in the way of certified law enforcement training, these volunteers have proven to be extremely effective in solving cyber crime cases.

In terms of leadership, training is critically needed to educate senior managers in law enforcement agencies about the utility and function of digital forensics investigations. This includes re-educating management about resourcing dependencies, the value of submitting devices for analysis, and tactical benefits associated with deploying specialist staff in the field (Blakey, 2000; Millen, 2000). Many policing agencies promote inexperienced supervisors into management positions in highly specialized units where teams are responsible for investigating cyber crime cases. In the absence of technical competencies needed to lead operations and supervise workflow, poorly selected managers will fail to account for staff welfare, negatively impact case outcomes, and ultimately undermine the credibility of the department or agency that they represent.

In the interests of promoting fairness, greater access to independent forensic facilities must be afforded to defendants whose cases are deemed significantly disadvantaged by the

expense of accessing forensic support. Funding for 'forensic aid' is crucial for under-resourced defendants, particularly when forensic evidence is a pivotal component of the prosecution's case against them. A threshold assessment regarding suitability for grant of forensic government assistance would need to be determined on a case-by-case basis by an independent and qualified body. When contesting cases in highly visible and politically charged circumstances, prosecutors within the adversarial system are usually at an advantage due to unimpeded access to forensic services and crime laboratories. Some commentators contend that "of all the disparities between defense and prosecution in the criminal justice system in the United States, that in the forensic field may be the greatest" (Kelly & Wearne, 1998, p. 15). One need only consider the injustice in the case of *R v Button* (2001) to exemplify how legitimate challenges to forensic evidence can overturn erroneous convictions.

Strong cryptography is indispensable to the success and development of an open system like the Internet. Evidently, the security safeguards implemented by powerful governments to protect highly sensitive and personally identifiable information (PII) are inadequate (Brown, 2015; Gallagher, 2015). Regardless of the proposed method of facilitating access to information on encrypted consumer devices, confidential data cannot be "kept secret from those with the skill to find and exploit the weak points, whether State or non-State, legitimate or criminal" (Office of the United Nations High Commissioner for Human Rights, p. 4). Intentionally compromising encryption within this volatile technological milieu, even for public interest justifications, weakens security and safety for everyone. Government regulation of cryptography undermines global cyber security, negatively impacts the public's perception about the integrity of police, inhibits cyber crime reporting, and results in the 'least trusted country' problem. Any limits on the strength of encryption, or concessions extended to investigating authorities by way of backdoors or 'master decryption keys', will result in a situation where the security of the international community is substantially weakened by the security posture adopted in the least trusted country. This is literally 'the weakest link' phenomenon manifested at the international level.

When nation-states throttle effective encryption, communication providers that comply with laws in those countries become compromised by association. Such an outcome also magnifies the problem of safe harbor for cyber crime offenders and opens the way to a burgeoning black market for crypto. Individually tailored solutions cannot be used at the executive level to impose weaknesses in encryption, even for exceptional cases. Rather, the judiciary must be the separate body empowered to severely reprimand those individuals and organizations who refuse to disclose decryption keys when compelled by a court of law. The author suggests that failure to provide the key to authorities investigating very serious crimes, for any reason, should be governed by the standard of strict liability, with a sliding scale of penalties. Offenders who are unable, or unwilling, to comply with court ordered decryption would receive 'punishment-in-default'. As such, sentencing would be commensurate with appropriate and applicable punitive measures or disciplinary actions, were the defendant to be found guilty of the charge or indictment leveled against them. The deterrence value of this approach is palpable and would certainly incentivize due diligence for individuals and organizations to implement safeguards to protect decryption keys. This strategy would also act as a potent 'reminder' for offenders and accomplices to provide the decryption passphrase for their data when law enforcement agencies have sufficient cause, and are legally empowered by a court of law,

to access this information as part of an investigation or prosecution. Whilst this solution may seem extremely coercive for individual suspects or defendants, the approach is far less totalitarian than the forcible methods currently tabled at the executive levels, which impact the collective security and safety of society as a whole. After all, why should many suffer for the crimes of a few?

Most importantly, there is a need to introduce uniform and thorough cyber crime reporting mechanisms. Various policing agencies globally are adopting strategies to encourage people to come forward, including awareness raising campaigns, web-based reporting portals, and cyber crime hotlines (Australian Communications and Media Authority, 2011). However, to adequately respond to reports of cyber crime, police must be equipped with the latest technology and be trained in industry best practices for handling ESI. A graduated response towards capacity building is also needed to ensure that probative sources of electronic evidence are discovered and preserved expeditiously. Pivotal to the success of cyber crime investigations and prosecutions is the development of in-house subject matter experts to run complex cases and direct technical inquiries (Dandurand, 2007). To build multidisciplinary teams, law enforcement agencies require increased training and procurement budgets and clear opportunities for career progression to encourage recruitment and retention of talent. To best assist fact-finders, courtrooms must be equipped with multimedia technology so that witnesses can effectively present results and convey meaning to essential aspects of the evidence. Lawyers, in particular, require practical understanding of the software used by police when processing ESI. A uniform taxonomy for criminal justice systems and legislative bodies is indispensable for achieving greater harmony among national and international legal frameworks (Giles & Hagestad II, 2013). Definitions of cyber crime offending must be expressed with precision, consistency, and formulated in consultation with the international community to be capable of overcoming language barriers and bridging cultural voids.

This research is predominantly based on materials written in English that are orientated towards the common law model of justice. Analysis of shared experiences regarding cyber crime offending in civil law countries and jurisdictions with legal systems that are not based on the common law tradition would be useful as a differentiator between systemic and technical barriers to justice. An emphasis on primary, first-hand source materials would also engender real-world insights into criminal justice responses to cyber crime. Further research on this topic would also add value by considering academic works and press articles published in languages other than English, including primary materials assembled from culturally diverse participants in criminal justice systems globally. In particular, extended scholarship on this topic might consider the micro-level causes and dynamic drivers, which encourage cyber crime offending. Analysis of a region's endowment with individuals possessing technical proficiency to exploit ICTs, push and pull factors which motivate movement of criminals into the underground economy, and the impact of organized criminal networks on cyber crime offending at the local level would be interesting from a threat intelligence perspective. A comprehensive approach will also yield wider perspectives from multinational stakeholders that may differ significantly from dominant western views within cyber crime and forensics discourses. After all "a society's power structure and the vested interests of powerful societal actors have an enormous impact on the way crimes in general and cybercrimes in particular are

defined, conceptualized, theorized, measured, responded to and policed" (Kshetri, 2010, p. 23).

Mary's Case: Acquittal

In his Chambers, the Judge orders that Lyon execute search and seizure warrants at Mary's address and specifies that an independent court-appointed expert perform forensic examination of any discovered devices. The Judge is highly critical of the testimony delivered by the Analyst from the e-Crime Unit.

A search of Mary's house is conducted a few days later. Police discover an intricate computer network consisting of both fixed and wireless devices. An Android hand-held device, as well as receipt for purchase of a Blackberry smart phone, matching the model owned by Paul, is also found. When asked about the whereabouts of the Blackberry, Mary dispassionately states that she lost the phone. Police also find a quantity of crushed hard disk drives in her basement. The drives are damaged beyond repair with no chance of data recovery.

Analysis of computers and network attached storage discovered at Mary's address shows that on each device the operating system and firmware has been refreshed. For those devices containing internal magnetic storage, it is apparent that new disk drives have been retrofitted. Similarly, examination of Mary's Android phone indicates that the device software has been reinstalled, including customized configuration for erasing historical content from the phone. When Lyon asks Mary why she engaged in this sweeping activity on her electronic devices she becomes very defensive and refuses to answer his questions, citing privacy concerns.

Paul is eventually acquitted of the charges and the investigation focusing on Mary is dropped for lack of evidence.

Conclusion

Leaders of industry are mindful of the need to ensure the resilience of their cyber defenses. Incident response and threat monitoring programs are developed; information security technologies are architected; and in-house lawyers specializing in data privacy law are retained. Physical and virtual security mechanisms are hardened and information systems rigorously probed for weaknesses by penetration testers. The agility and capability of the Security Operations Center (SOC) is assessed using cyber war-gaming exercises which gauge effectiveness of reactive and proactive defenses to advanced persistent adversaries (Brown, 2015). These shrewd defensive measures are crafted to detect, mitigate and contain the gamut of technical, legal and reputational risks facing an enterprise and its clients. As information system vulnerabilities are exposed, patches are applied. If gaps in knowledge are detected, education is provided. Should user behavior require modification, policies are drafted and implemented. When indicators of compromise (IOCs) are detected, countermeasures are triggered and actioned.

In contrast, governments worldwide have shown marked reluctance to scrutinize the effectiveness of state-controlled mechanisms for investigating and prosecuting serious instances of cyber crime offending. More than a decade ago, Susan Brenner contended that the "justice system's inability to prosecute cybercrime cases is a sign that it is not functioning effectively in this area" (Brenner, 2004, p. 81). This in-depth research reveals that Brenner's assertion is as relevant today as it was back then. A combination of factors has converged to impede criminal justice processes in common law countries worldwide. Nation-states, including private sector entities, police departments, and academic

institutions, have shared with the United Nations their experiences and concerns (United Nations Office on Drugs and Crime, 2013). In order to overcome barriers to investigations and prosecutions targeting cyber crime offending, solutions are urgently needed. *Table 8* highlights the primary challenges presented by cyber crime for the administration of criminal justice.

Table 8. Barriers to Cyber Crime Investigations, Prosecutions, and Digital Forensics Interrogations

Category	Description
Identification	• Difficulty in attributing ownership and authorship to electronically stored information. • Difficulty in identifying individuals in control of information systems and devices. • Inability to expediently locate relevant information amongst large sets of data. • Ineffectiveness in tracing criminal activity when data anonymization and obfuscation techniques have been employed. • Widespread availability of data sanitization and device wiping software for consumer devices which may lead to destruction of evidence.
Access	• Inability to obtain authorization for conducting online inspection and collection of remotely stored data, particularly if the target host is a cloud service provider with a base of operations outside the jurisdiction of local authorities. • Delays in processing requests for Mutual Legal Assistance due to bureaucratic stumbling blocks. • Inability to acquire data due to advancements in consumer security on commodity devices, including strong encryption, open source privacy tools, and anti-forensics technologies. • Legislation which compels manufacturers and service providers to give investigating authorities access to electronically stored information is becoming redundant. Companies are relinquishing the means to unlock devices and decode data. It is technically infeasible for courts to compel foreign manufactures to create keys to comply with local laws. • Penalties imposed by courts in circumstances where defendants refuse to comply with orders to disclose decrypted data are ineffective. Where serious criminal offending is involved, an offender is unlikely to turn over the key to incriminating data, particularly if the punishment for contempt of court is less than the crime for which they are being tried.
Wellbeing	• High performance pressure and stressful working conditions for criminal justice officers may lead to staff burnout. • Prolonged exposure to obscene material may create mental health issues for investigators, prosecutors, and forensic interrogators. • Staff welfare may be overlooked and investigations derailed in policing environments when non-technical managers are appointed to supervisory positions without substantive experience overseeing cyber crime inquiries or attending to the rigors of digital forensic casework.
Liability	• Interference with commercial operations when warrant activity is executed in business environments may lead to substantial claims for damages. • Unintended damage to information systems and devices when investigators seize exhibits or perform analysis on commercial equipment may expose law enforcement agencies to civil litigation. • Disclosure of private, confidential, or legally privileged information during an investigation may lead to criminal, civil and/or internal administrative legal proceedings for criminal justice officers and departments involved.

Policies and processes	• Willingness of law enforcement agencies to commit resources to cyber crime offending may depend on the extent to which an investigation or prosecution is congruent existing with policy preferences, public priorities, or political agendas. • Documented operating procedures are necessary to guide handling of electronic evidence by investigating authorities. When this documentation is not available for inspection during legal proceedings, serious questions may be raised about the consistency and transparency of internal police processes.
Retrieval and retention	• Ephemeral or volatile sources of electronic information which is not collected from live systems during warrant activity may substantially weaken a case in the eyes of the court, or lead to miscarriages of justice. • Service providers who do to respond to authorized requests for production and preservation of data may cause the loss of critical evidence.
Admissibility and fairness	• Chain-of-custody documentation which is incomplete or inaccurate may result in electronic evidence being classified as inadmissible. • Law enforcement agencies who are unable to attest to the reliability or authenticity of electronic information may thwart the efforts of legal counsel to introduce that material as evidence in court. • Investigating authorities and experts witnesses who exhibit insufficient objectivity may weaken the credibility of evidence that is presented in court. • Analysts and investigators who are unable to dedicate time towards identifying exculpatory sources of evidence may undermine the strength of a case or cause miscarriages of justice. • Defendants that are unable to afford forensic support to test investigative findings and challenge expert opinion may be wrongly convicted.
Human capital	• Law enforcement officers and prosecutors without the technical expertise needed to manage cyber crime cases may contribute towards the acquittal of cyber crime offenders which pose a substantial threat to public safety. • Analysts who are not qualified to operate technical equipment or extract data from information systems may contaminate evidence and severely undermine the credibility forensic reports led in support of police investigations. • Agencies without sufficient in-house subject matter expertise will undermine the ability of prosecutors to introduce expert evidence that explains the technical underpinnings and relevance of material before the court.
Technical resources and funding	• Police who are not equipped with specialized tools for extracting information, or furnished with sufficient computational power to expediently process data, may miss critical evidence during analysis in the laboratory or while performing triage in the field. • Court rooms that are not fitted with modern technology required to effectively present electronic evidence during legal proceedings may degrade the clarity and persuasiveness of testimony.
Training	• Police officers, prosecutors, and members of the judiciary that are not provided with ongoing training which is focused on modes of criminal offending, diplomatic channels of cooperation, foreign mechanisms of justice, sovereignty issues, emerging sources of electronic information, and communication technologies more generally, will be manifestly ill-equipped to manage cyber crime cases.

Underreporting and uncertainty	• Public misconceptions about the capacity of police to target cyber crime offending contributes to the problem of underreporting. • Gaps in legislation, and administrative delays owing to judicial uncertainty about the nature of cyber crime offending, may prevent investigators from obtaining requisite legal authority to intercept electronic data. • Defense counsel may seek to create confusion in the mind of an inexperienced judge or juror by raising nebulous legal and technical arguments to derail the prosecution's case. • Expert witnesses may mislead the trier of fact by overstating or understating findings.
Privacy and privilege	• Investigations may infringe upon fundamental human rights and lead to accountability failure if the judiciary is not sufficiently empowered to provide oversight. • Doctrine of legal professional privilege may delay investigations and add a layer of complexity to forensic interrogations and legal process. • Emerging data protection and privacy laws worldwide are putting electronic information beyond the reach of investigating authorities.
Cooperation	• Private sector entities that are slow in responding to requests for assistance or from police, or are generally dismissive of collaborative initiatives with law enforcement agencies, create barriers to cyber crime investigations, prosecutions, and digital forensics interrogations. • Strict and formal international mechanisms of cooperation may impede the agility of police investigations which target cyber crime offending originating outside national borders.
Legal frameworks and due process	• Legislative provisions which are not harmonized among members of the international community may create safe jurisdictions for cyber crime offending, and possible conflicts of law. • Laws that are not drafted to encompass technology broadly within established categories of criminal conduct will rapidly become obsolete, thereby impeding the capacity of authorities to lead cyber crime investigations and run effective prosecutions. • Legislative time constraints pertaining to the examination of data on information systems may be insufficient given exponential increases in consumer storage capacity and the complexity of extracting records from devices. Consequently, large quantities of data seized by police may never be analyzed.

As society evolves and technology marches forward our understanding of the origins of criminality must be continuously revised. The persistence, prevalence and seriousness of cyber crime offending demands a greater response from the international community. Technology is now deeply enmeshed within the fabric of society. Criminals understand that technology is a highly effective force multiplier which can be abused to enable illicit activity, and leveraged to facilitate access to a global constituency of victims living online. Our collective dependency on technology makes this threat extremely difficult to eliminate. The relative ease with which offenders engage in cyber crime, and the high gains afforded to perpetrators, ensures that motivation for reprobates and recidivists remains strong. Manifestations of crime emanating from the cyber domain are among the most formidable challenges for workers in criminal justice systems worldwide. The magnitude of this challenge is clearly acknowledged by the US Intelligence Community who classify 'cyber' as the prime global threat to national security, ahead of 'terrorism', 'proliferation of weapons of mass destruction', and 'transnational organized crime' (Clapper, 2015). The status quo has now reached a critical tipping point where proactive

measures must be actioned to raise awareness, identify barriers, and counter a growing threat which is highly organized, well-funded, and immensely lucrative.

References

Acharya, M. P. (2013, November). The Adversarial v. Inquisitorial Models of Justice. *KSL Journal*, *1*, 63-70. Retrieved on 11th November 2014 from http://ksl.edu.np/cpanel/pdf/adversial.pdf.

Adams, D. (2003, December 16). Police prove a match for electronic foe. *The Sydney Morning Herald*. Retrieved on 28th January 2015 from http://www.smh.com.au/articles/2003/12/15/1071336882279.html?from=storyrhs.

Akin, T. (2011). Cybercrime: Response, investigation, and prosecution. *Encyclopedia of Information Assurance* (pp. 749-753). New York: Taylor and Francis.

Alghafli, K. A., Jones, A., & Martin, T. A. (2011).Guidelines for the digital forensic processing of smartphones. *9th Australian Digital Forensics Conference*, SECAU Security Research Centre, Edith Cowan University, Perth, Western Australia. Retrieved on 7th November 2014 from http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1089&context=adf.

Allen, G. (2005). Responding to cybercrime: A delicate blend of the orthodox and the alternative. *New Zealand Law Review*, *2*, 149-178.

Allison, R. (2003, October 18). Youth cleared of crashing American port's computer. *The Guardian*. Retrieved on 9th November 2014 from http://www.guardian.co.uk/technology/2003/oct/18/uknews.onlinesupplement.

American Convention on Human Rights (1969).

Anderson, D. (2015, June 11). A Question of Trust – Report of the Investigatory Powers Review. *Independent Reviewer of Terrorism Legislation*. Retrieved on 11th June 2015 from https://terrorismlegislationreviewer.independent.gov.uk/a-question-of-trust-report-of-the-investigatory-powers-review/

Anonymous (2015, June 20). Quantum computers - A little bit, better. *The Economist*. Retrieved on 21st June 2015 from http://www.economist.com/news/science-and-technology/21654566-after-decades-languishing-laboratory-quantum-computers-are-attracting.

Apple (2015, April). iOS Security: iOS 8.3 or later. *iOS Security Guide White Paper*. Retrieved on 3rd June 2015 from https://www.apple.com/business/docs/iOS_Security_Guide.pdf.

Arms, W. Y. (2000). *Digital Libraries*. London: MIT Press.

Ashford, W. (2015, June 3). Law enforcement officers weigh in on encryption at Infosecurity Europe. *ComputerWeekly.com*. Retrieved on 12th March 2015 from http://www.computerweekly.com/news/4500247458/Law-enforcement-officers-weigh-in-on-encryption-at-Infosecurity-Europe.

Association of Chief Police Officers (2007, August 7). *Good practice guide for computer-based electronic evidence*. Retrieved on 11th November 2014 from http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf.

Association of Chief Police Officers (2009). *ACPO e-crime strategy*. Retrieved on 7th November 2014 from http://itlaw.wikia.com/wiki/ACPO_e-Crime_Strategy.

Australian Communications and Media Authority (2011, May).*An overview of international cyber-security awareness raising and educational initiatives*. Retrieved on 5th November 2014

from http://www.acma.gov.au/webwr/_assets/main/lib310665/galexia_report-overview_intnl_cybersecurity_awareness.pdf.

Australian Government (2012, July). *Equipping Australia against emerging and evolving threats*. Attorney-General's Department, Canberra. Retrieved on 11th November 2014 from http://www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=pjcis/nsl2012/additional/discussion%20paper.pdf.

Australian Institute of Criminology (2011, July 18). Definitions and general information. *Australian Government*. Retrieved on 8th November 2014 from http://www.aic.gov.au/crime_types/cyber crime/definitions.html.

Ballin, H., & Ballin, M. F. H. (2012). *Anticipative criminal investigation - Rule of law principles for counterterrorism*. The Hague, Netherlands: T.M.C. Asser Press.

Banks, A. (2014, November 10). Stop and Search Under Fire. *The Western Australian*. Retrieved on 11th November 2014 from http://au.news.yahoo.com/thewest/a/-/newshome/7564062/stop-and-search-laws-under-fire/.

Barlow, J. P. (1992). Decrypting the puzzle palace. *Communications of the ACM*, *35*(7), 25-31.

Barrett, J., & Kippler, G. (2010). *Virtualization and Forensics: A digital forensic investigator's guide to virtual environments*. Boston: Syngress.

Bennett, D. (2012). The Challenges Facing Computer Forensics Investigators in Obtaining Information from Mobile Devices for Use in Criminal Investigations. *Information Security Journal: A Global* Perspective, *21*(3), 159-168.

Berger v New York, 388 US 41 (1967).

Bermay, F. P., & Godlove, N. (2012). Understanding 21st century cybercrime from the 'common' victim'. *Criminal Justice Matters*, *89*(1), 4-5.

Bhattacharjee, Y. (2011, January 31). How a remote town in Romania has become cybercrime central. *Wired*. Retrieved on 10th November 2014 from http://www.wired.com/magazine/2011/01/ff_hackerville_romania/all/.

Biggs, S., & Vidalis, S. (2009, November 9-12). Cloud computing: the impact on digital forensic investigations. Paper presented at the *International Conference for Internet Technology and Secured Transactions (ICITST)*. IEEE (pp. 1-6).

Blakey, D. (2000). *Under the Microscope: Thematic Inspection Report on Scientific and Technical Support*. Her Majesty's Inspectorate of Constabulary, United Kingdom.

Bocij, P., & McFarlane, L. (2003). Cyberstalking: The technology of hate. *The Police Journal*, *76*, 204-221.

Bologna, G. J., & Lindquist, R. J. (1987). *Fraud Accounting and Forensic Accounting – New Tools and Techniques*. Brisbane: John Wiley & Sons.

Bowling, B., & Foster, J. (2002). Policing and the Police. In M. Maguire, R. Morgan & R. Reiner (Eds.), *The Oxford Handbook of Criminology*, 3rd edition. Oxford: Oxford University Press.

Boyle. J. (2007). Foucault in cyberspace: Surveillance, sovereignty, and hardwired censors. *University of Cincinnati Law Review*, *66*(1), 178-183.

Brenner, S. Carrier, B., & Henninger, J. (2004). The Trojan Horse Defense in Cyber crime Cases. *Santa Clara Computer and High Technology Law Journal*, *21*, 1-53.

Brenner, S. W. (2004). Toward a Criminal Law for Cyberspace: A New Model of Law Enforcement? *Rutgers Computer and Technology Law Journal*, *30*, 1-104.

Brenner, S. W. (2008). *Cyberthreats: The Emerging Fault Lines of the Nation State*. New York: Oxford University Press.

Brenner, S. W., & Koops, B.-J. (2004). Approaches to cyber crime jurisdiction. *Journal of High Technology Crime*, *15*(1), 1-46.

Broadhurst, R. G. (2006). Developments in the global law enforcement of cyber-crime. *Policing: an International Journal of Police Strategies and Management*, *29*(3), 408-433.

Broadhurst, R. Grabosky, P., Alazab, M., & Chon, S. (2014). Organizations and Cyber Crime: An Analysis of the Nature of Croups engaged in Cyber Crime. *International Journal of Cyber Criminology*, *8*(1), 1-20. Retrieved on 22nd February 2015 from http://www.cybercrimejournal.com/broadhurstetalijcc2014vol8issue1.pdf.

Broadhurst, R., & Davies, S. E. (Eds.) (2009). *Policing in Context: An introduction to Police Work in Australia*, South Melbourne, Victoria: Oxford University Press.

Bromby, M. (2006). Security against Crime: Technologies for Detecting and Preventing Crime. *International Review of Law Computers & Technology*, *20*, 1-5.

Brown, C. S. D. (2015). Cyber-Attacks, Retaliation and Risk: Legal and Technical Implications for Nation-States and Private Entities. In J. L. Richet (Ed.), *Cybersecurity Policies and Strategies for Cyberwarfare Prevention* (pp. 166-203). Hershey, PA: IGI Global.

Buchholz, F., & Tjaden, B. (2007). A brief study of time. *Digital Investigation, 4*, 31-42.

Caltagirone, S. (2015, May 22). The Cost of Bad Threat Intelligence. *ActiveResponse.org*. Retrieved on June 10th2015 from http://www.activeresponse.org/the-cost-of-bad-threat-intelligence.

Caproni, V. (2011, February 11). Going Dark: Lawful Electronic Surveillance in the Face of New Technologies. Statement by Valerie Caproni, General Counsel Federal Bureau of Investigation, before the *House Judiciary Committee, Subcommittee on Crime, Terrorism, and Homeland Security*, Washington, D.C. Retrieved on 14th June 2015 from https://www.fbi.gov/news/testimony/going-dark-lawful-electronic-surveillance-in-the-face-of-new-technologies.

Carrier, B. D. (2006). Risks of Live Digital Forensic Analysis. *Communications of the ACM*, *49*(2), 56-61.

Casey, E. (2002). Error Uncertainty and Loss in Digital Evidence. *International Journal of Digital Evidence*, *1*(2). Retrieved on 2nd November 2014 from https://utica.edu/academic/institutes/ecii/publications/articles/A0472DF7-ADC9-7FDE-C80B5E5B306A85C4.pdf.

Casey, E. (2004). *Digital Evidence and computer crime: Forensic Science, computers and the Internet*, second edition. London: Elsevier Academic Press.

Cassese, A. (2003). Is the Bell Tolling for Universality? A Plea for a Sensible Notion of Universal Jurisdiction. *Journal of International Criminal Justice*, *1*(3), 589-595.

Caulfield, C., & Buttler, M. (2003, January 31). Poison water threat – Cyanide scare man charged. *Herald Sun*.

Chaikin, D. (2006). Network investigations of cyber attacks: the limits of digital evidence. *Crime, Law and Social Change*, *46*, 239-256.

Charter of Fundamental Rights of the European Union (2000).

Charter of Human Rights and Responsibilities Act (2006) (Victoria).

Charter of the United Nations (1945).

Chaski, C. E. (2005). Who's At The Keyboard? Authorship Attribution in Digital Evidence Investigations. *International Journal of Digital Evidence*, *4,* 1-13. Retrieved on 27th October 2014 from

http://www.utica.edu/academic/institutes/ecii/publications/articles/B49F9C4A-0362-765C-6A235CB8ABDFACFF.pdf.

Chen, A. (2015, June 2). The Agency. *The New York Times Magazine*. Retrieved 9th June 2015 from http://www.nytimes.com/2015/06/07/magazine/the-agency.html?_r=0.

Chik, W. B., & Bartholomew, W. (2011). Challenges to Criminal Law Making in the New Global Information Society: A Critical Comparative Study of the Adequacies of Computer-Related Criminal Legislation in the United States, the United Kingdom and Singapore. Retrieved on 10th November 2014 from http://www2.law.ed.ac.uk/ahrc/complaw/docs/chik.doc.

Chong, S. (2012, October). A Walk In The Clouds: Meeting the Challenges of Cloud Computing. Remarks by Singapore Attorney-General Steven Chong, S.C. at the *17th Annual Conference of the International Association of Prosecutors*. Retrieved 14th June 2015 from http://www.iap-association.org/Conferences/Annual-Conferences/17th-Annual-Conference-and-General-Meeting,-Bangko/WS1A_speech_Steven_Chong_FINAL.aspx.

Clancy, T. K. (2011). *Cyber Crime and Digital Evidence: Materials and Cases*. New York: Matthew Bender & Company, Inc.

Clapper, J. R. (2015, February 26). Worldwide Threat Assessment of the US Intelligence Community. Statement for the record by James R. Clapper, Director of National Intelligence, for the *Senate Armed Services Committee*. Retrieved 16th June 2015 from http://www.dni.gov/files/documents/Unclassified_2015_ATA_SFR_-_SASC_FINAL.pdf.

Clarke, R. V. (2004). Technology, Criminology and Crime Science. *European Journal on Criminal Policy and Research*, *10*, 55–63.

Cloud Security Alliance (2010, March). Top Threats to Cloud Computing V1.0. *Cloud Security Alliance*. Retrieved on 18th October 2014 from https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf.

Clough, J. (2011). Cybercrime. *Commonwealth Law Bulletin*, *37*(4), 671-680.

Code of Criminal Procedure (2000) (France).

Collier, P. A., & Spaul, B. J. (1992, June). Problems in Policing Computer Crime. *Policing & Society*, *2*(4), 307-320.

Comey, J. B. (2014, October 16). Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course? Speech by James B. Comey, Director Federal Bureau of Investigation, to *Brookings Institution*, Washington, D.C. Retrieved on 11th June 2015 from https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course.

Commonwealth Internet Governance Forum (2012, December 20). Child Pornography: Model Legislation and Global Review. *Blog*. Retrieved on 9th November 2014 from http://www.commonwealthigf.org/blog/update-child-pornography-model-legislation-and-global-review/.

Commonwealth Model Law on Computer and Computer Related Crime (October 2002).

Communications Assistance for Law Enforcement Act (1994).

Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families (1990).

Convention on the Rights of Persons with Disabilities (2006).

Convention on the Rights of the Child (1989).

Cordero, C. & Zwillinger, M. (2015, April 19). Should Law Enforcement Have the Ability to Access Encrypted Communications? *The Wall Street Journal*. Retrieved on June 11th 2015 from http://www.wsj.com/articles/should-law-enforcement-have-the-ability-to-access-encrypted-communications-1429499474.

Council of Europe Convention on Cybercrime (2001), and *Additional Protocols* (2003).

Council of Europe Treaty Office (2015, February 28). Convention on Cybercrime. CETS No.: 185. Retrieved on 8th June 2015 from http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CL=ENG.

Council of the European Union, *Council Act of 26 July 1995* drawing up the Convention on the establishment of a European Police Office (Europol Convention).

Council of the European Union, *Council Framework Decision 2004/68/JHA*.

Council of the European Union, *Council Framework Decision 2005/222/JHA*.

Council of the European Union, *Data Retention Directive 2005/0182/COD*.

Council of the European Union, *Directive on Child Pornography 2011/92/EU*.

Court of Justice of the European Union (2014, April 8). The Court of Justice declares the Data Retention Directive to be invalid. *PRESS RELEASE No 54/14, Judgment in Joined Cases C-293/12 and C-594/12*. Retrieved 12th June 2015 from http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf.

Crimes Act (1914) (Commonwealth).

CrowdStrike (2015, February 9). 2014 Global Threat Intel Report. *CrowdStrike Threat Intel*. Retrieved 10th June 2015 from http://go.crowdstrike.com/rs/crowdstrike/images/GlobalThreatIntelReport.pdf.

Cybercrime Act (2001) (Commonwealth).

Davis, J. H. (2015, July 9). Hacking of Government Computers Exposed 21.5 Million People. *The New York Times*. Retrieved 5th August 2015 from http://nyti.ms/1HiFLCZ.

D'Ovidio, R., & Doyle J. (2003). A study on Cyberstalking: Understanding investigative hurdles. *FBI Law Enforcement Bulletin*, *72*(3), 10-17.

Dandurand, Y. (2007). Strategies and practical measures to strengthen the capacity of prosecution services in dealing with transnational organized crime, terrorism and corruption. *Crime, Law and Social Change*, *47*, 225-246.

Davidoff, S., & Ham, J. (2012). *Network Forensics - Tracking Hackers Through Cyberspace*. Upper Saddle River, NJ: Pearson Education, Inc.

Davies, M. (1999, December 12). Failing to Deliver on Cyber Crime. *Birmingham Post*.

Dee, M. (2012). Getting back to the Fourth Amendment: Warrantless cell phone searches. *New York Law School Law Review*, *56*, 1129-1163. Retrieved on 26th February 2015 from http://www.nylslawreview.com/wp-content/uploads/sites/16/2012/02/Dee-note.pdf.

Dell SecureWorks (2015, June 15). Stegoloader: A Stealthy Information Stealer. *Dell SecureWorks Counter Threat Unit Threat Intelligence*. Retrieved 16th June 2015 from http://www.secureworks.com/cyber-threat-intelligence/threats/stegoloader-a-stealthy-information-stealer/.

Denning, D. E. (2001). Activism, hacktivism, and cyberterrorism: The Internet as a Tool for Influencing Foreign Policy. In J. Arquilla & D. F. Ronfeldt (Eds.), *Networks and Netwars: The Future of Terror, Crime, and Militancy* (pp. 239–288). Santa Monica: RAND.

Denning, D. E., & Baugh Jr, W. E. (1999). Hiding Crimes in Cyberspace. *Information, Communication & Society*, *2*(3), 251-276.

Di Gregory, K. V. (2000, September 7). Foreign ownership of American Telecommunications Companies. Statement before the US House of Representatives Subcommittee on Telecommunications, Trade, and Consumer Protection Committee on Commerce. Retrieved on 10th November 2014 from http://www.gpo.gov/fdsys/pkg/CHRG-106hhrg67113/html/CHRG-106hhrg67113.htm.

Doe v United States, 805 F. Supp. 1513 (D. Hawaii. 1992).

Downing, R. W. (2005). Shoring Up the Weakest Link: What Lawmakers Around the World Need to Consider in Developing Comprehensive Laws to Combat Cybercrime. *Columbia Journal of Transnational Law*, *43*, 741-762.

Dubord, P. (2008). Investigating Cybercrime. In J. J. Barbara (Ed.), *Handbook of Digital and Multimedia Forensic Evidence* (pp. 77-89). Totowa, NJ: Humana Press Inc.

Eckert, W. G. (1980). Coordination of forensic activities and use in court. In W. G. Eckert (Ed.), *From Introduction to Forensic Sciences* (pp. 205-212). St. Louis, Missouri: The C. V. Mosby Company.

Eckert, W. G. (Ed.) (1997). *Introduction to Forensic Sciences*, 2nd edition. New York: Elsevier.

Edelmann, R. J. (2010). Exposure to child abuse images as part of one's work: Possible psychological implications. *Journal of Forensic Psychiatry & Psychology*, *21*(4), 481-489.

Editorial Board (2014, October 3). Compromise needed on smartphone encryption. *The Washington Post*. Retrieved on 10th June 2015 from http://www.washingtonpost.com/opinions/compromise-needed-on-smartphone-encryption/2014/10/03/96680bf8-4a77-11e4-891d-713f052086a0_story.html.

Endgame (2015, April 16). Turn the map around to prevent damage and loss from cyber attack. *Endgame White Paper*. Retrieved on 4th June 2015 from http://pages.endgame.com/WC2015-04EnterpriseWhitepaper_WCYYYYMMDDWebContent.html.

European Convention for the Protection of Human Rights and Fundamental Freedoms (1953).

European Convention on Human Rights (1950).

European Convention on Mutual Assistance in Criminal Matters (1959).

European Parliament and of the Council, *Directive 2006/24/EC*.

Farivar, C. (2015, May 12). Cops must now get a warrant to use stingrays in Washington State. *Ars Technica*. Retrieved on 10th June 2015 from http://arstechnica.com/tech-policy/2015/05/cops-must-now-get-a-warrant-to-use-stingrays-in-washington-state/.

Field, D., Coyle, I. R., Starmer, G. A., Miller, G., & Wilson, P. (2009). Trust me – I'm an expert: forensic evidence and witness immunity. *Australian Journal of Forensic Sciences*, *41*(2), 113-129.

Findlay, M. (2004). *Introducing Policing: Challenges for Police and Australian Communities*. Melbourne: Oxford University Press.

Finn, J. & Banach, M. (2000). Victimization online: The down side of seeking human services for women on the Internet. *Cyber Psychology& Behaviour*, *3*(2), 243-254.

FireEye Labs (2015, April 15). APT30 and the mechanics of a long-running cyber espionage operation. *FireEye Threat Intelligence Special Report*. Retrieved 5th May 2015 from https://www2.fireeye.com/rs/fireye/images/rpt-apt30.pdf.

Fisher, D. (2015, April 30). Congress, Crypto, and Craziness. *Threat Post*. Retrieved on 12th June 2015 from https://threatpost.com/congress-crypto-and-craziness/112508.

Flatman, G. (2004, January 16). DNA: A Trial Lawyer's Perspective. Retrieved 21st October 2014 from http://www.aic.gov.au/media_library/conferences/medicine/flatman.pdf.

Foreign Intelligence Surveillance Act (1978).

Forte, D. (2006). Advances in Onion Routing: Description and backtracing/investigation problems. *Digital Investigation*, *3*, 85-88.

Fowler v Padget (1798) 7 TR 509; 101 ER 1103.

Freckelton, I., & Selby, H. (2005). *Expert Evidence: Law, Practice, Procedure and Advocacy*, 3rd edition. Sydney: Lawbook Company.

Freckelton, I., Reddy, P., & Selby, H. (1991). *Australian Judicial Perspectives on Expert Evidence: An Empirical Study*. Victoria: AIJA.

Freckelton, I., Reddy, P., & Selby, H. (2001). *Australian Magistrates' Perspectives on Expert Evidence: A Comparative Study*. Victoria: AIJA.

Frolova, I. (2011, January 31). Real punishment for virtual criminals. *Voice of Russia*. Retrieved on 3rd November 2014 from http://sputniknews.com/voiceofrussia//2011/01/31/42167678/.

Gallagher, S. (2015, June 16). Encryption "would not have helped" at OPM, says DHS official. *Ars Technica*. Retrieved on 17th June 2015 from http://arstechnica.com/security/2015/06/encryption-would-not-have-helped-at-opm-says-dhs-official/.

Garland, D. (2001). *The culture of control: crime and social order in society*. Chicago: The University of Chicago Press.

Geist, M. (2003). Cyber Law 2.0. *Boston College Law Review*, *44*(2), 359-396.

Gercke, M. (2012). Hard and soft law options in response to cybercrime - How to weave a more effective net of global responses. *Computer Law Review International*, *3*, 78-87.

Ghosh, S. (2002). *Principles of secure network systems design*. New York: Springer.

Gianarelli v Wraith (1988) 165 CLR 543.

Gilbert, J. N. (2004). *Criminal Investigations*, 6th edition. Upper Saddle River, New Jersey: Pearson Education, Inc.

Giles, K., & Hagestad II, W. (2013). Divided by a Common Language: Cyber Definitions in Chinese, Russian and English. Paper presented at the *5th International Conference on Cyber Conflict*, NATO Tallinn.

Gill, P., & Phythian, M. (2012). *Intelligence in an Insecure World*, 2nd edition. Cambridge, UK: Polity Press.

Girodo, M., Deck, T., & Morrison, M. (2002). Dissociative-type identity disturbances in undercover agents: Socio-cognitive factors behind false-identity appearances and reenactments. *Social Behavior and Personality*, *30*, 631-644.

Gold, V. (1992, June 13). If All Fails, Read the Instructions. *New Scientist*, *1825*, 38-41.

Goodman, M. (2011, November). What Business Can Learn from Organized Crime. *Harvard Business Review*. Retrieved on 13th June 2015 from https://hbr.org/2011/11/what-business-can-learn-from-organized-crime.

Goodman, M. D. (1997). Why The Police Don't Care About Computer Crime. *Harvard Journal of Law & Technology*, *10*(3), 466-495.

Goodman, M. D., & Brenner, S. W. (2002). The Emerging Consensus on Criminal Conduct in Cyberspace. *International Journal of Law and Information Technology*, *10*(2), 139-223.

Goodman, S. E., & Sofaer, A. D. (Eds.) (2001). *The Transnational Dimension of Cyber Crime and Cyber Terrorism*. Stanford: Hoover Institution Press.

Goodno, N. H. (2007). Cyberstalking, a New Crime: Evaluating the Effectiveness of Current State and Federal Laws. *Missouri Law Review*, *72*, 125-196.

Gordon S., & Ford, R. (2006). On the Definition and Classification of Cyber crime. *Journal of Computer Virology*, *2*(1), 13-20.

Grabosky, P. (2007). Requirements of prosecution services to deal with cyber crime. *Crime, Law and Social Change*, *47*, 201-223.

Grace T., & Mell, P. (2011, September). The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology. NIST Special Publication, No 800-145. National Institute of Standards and Technology: United States Department of Commerce. Retrieved on 16th February 2015 from http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

Graham, J., Howard, R., & Olson, R. (Eds.) (2011). *Cyber Security Essentials*. Boca Raton: Taylor and Francis Group.

Graycar, A. (2001, June 21-22). New crimes or new responses. Speech presented at 4th National Outlook Symposium on Crime in Australia: New Crimes or New Responses. Canberra: Rydges Lakeside.

Haagman, D., & Ghavalas, B. (2005). Trojan defence: A forensic view. *Digital Investigation*, *2*, 22-30.

Hall, J. L (2015, April 20). The NSA's Split-Key Encryption Proposal is Not Serious. *Center for Democracy and Technology*. Retrieved on 12th June 2015 from https://cdt.org/blog/the-nsas-split-key-encryption-proposal-is-not-serious/.

Hamer, M. (1992). Forensic Science Goes on Trial. *New Scientist*, *132*(1794), 30-33.

Harris v Smith, 372 F.2d (8th Cir 1967).

Hay, B., Nance, K., & Bishop, M (2009, March). Live Analysis: Progress and Challenges. *IEEE Security and Privacy*, 7(2), 30–37.

Herrera-Flanigan, J. R., & Ghosh, S. (2010). Criminal Regulations. In S. Ghosh & E. Turrini (Eds.), *Cybercrimes: A Multidisciplinary Analysis*, (pp. 265-308). Berlin: Springer.

Hodgson, J. S. (2010). The Future of Adversarial Criminal Justice in 21st Century Britain. *North Carolina Journal of International Law and Commercial Regulation*, *35*, 319-362.

Holt, T. J. (2012). Exploring the Intersections of Technology, Crime, and Terror. *Terrorism and Political Violence*, *24*(2), 337-354.

Holt, T. J., & Blevins, K. R. (2008). Examining the Stress, Challenges, and Experiences of Forensic Examiners. Paper presented at the annual meetings of the *Southern Criminal Justice Association*, New Orleans, LA.

Horswell, J. (2004). Crime scene investigation and third party quality systems accreditation: Australia's experience. In J. Horswell (Ed.), *The Practice of Crime Scene Investigation*. Boca Raton: CRC Press.

Huber, M., Mulazzani, M., Leithner, M., Schrittwieser, S., Wondracek, G., & Weippl, E. (2011). Social snapshots: digital forensics for online social networks. Paper presented at *Annual Computer Security Applications Conference – ACSAC 2011*, Orlando, Florida,

USA. Retrieved on 11th November 2014 from http://publik.tuwien.ac.at/files/PubDat_202726.pdf.

Hughes v United States, 953 F.2d 531 (9th Cir. 1992).

Hughes, J. (2003). The Internet and the Persistence of Law. *Boston College Law Review*, *44*(2), 359-396.

Hunton, P. (2011). The stages of cybercrime investigations: Bridging the gap between technology examination and law enforcement investigation. *Computer Law & Security Review*, *27*, 61-67.

Husain, M. I., & Sridhar, R. (2010). iForensics: Forensic Analysis of Instant Messaging on Smart Phones. *Digital Forensics and Cyber Crime - Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, *31*, 9-18.

Inter-American Convention on Mutual Assistance in Criminal Matters (1992, Treaty Series, OAS, No. 75).

International Covenant on Civil and Political Rights (1966).

International Telecommunications Union (2009, April).Understanding Cyber crime: A Guide for developing countries page. ITU Cyber crime Legislation Resources, ICT Applications and Cybersecurity Division Policies and Strategies Department. Retrieved on 17th October 2014 from http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-understanding-cyber crime-guide.pdf.

International Telecommunications Union (2012). *Understanding Cyber crime* – Phenomena, Challenges, Legal Response, 2nd edition. Retrieved on 7th November 2014 from http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cyber crime%20legislation%20EV6.pdf.

Jarrett, H. M., & Hagen, E. (2009, July). Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations. United States Department of Justice, Office of Legal Education Executive Office for United States Attorneys. Retrieved on 6th November 2014 from http://www.justice.gov/criminal/cyber crime/docs/ssmanual2009.pdf.

Jasanoff, S. S. (1995). *Science at the Bar*. Cambridge Massachusetts: Harvard University Press.

Jones, R. (2006). Your day in court – the role of the expert witness. *Digital Investigation*, *1*, 273-278.

Julian, R. D., Kelty, S. F., Roux, C., Woodman, P., Robertson, J., Davey, A., Hayes, R., Margot, P., Ross, A., Sibly, H., & White, R. (2011). What is the value of forensic science? An overview of the effectiveness of forensic science in the Australian criminal justice system project. *Australian Journal of Forensic Sciences*, *43*(4), 217-229.

Kaspersen, H. W. K. (1995). Computer related crime, information security and investigation of crime: A delicate triangle. *International Review of Law, Computers & Technology*, *9*(1), 129-141.

Kaspersky Lab (2015, February 16). Carbanak APT: The Great Bank Robbery. *Securelist*. Retrieved on 26th February 2015, from https://securelist.com/files/2015/02/Carbanak_APT_eng.pdf.

Katz v United States, 839 US 347 (1967).

Kaye, B. H. (1995). *Science and the Detective – Selected Reading in Forensic Science*. New York: VCH Verlagsgesellschaft.

Kelly J. F., & Wearne, P. K. (1998). *Tainting Evidence: Inside the Scandals at the FBI Crime Lab*. Sydney: The Free Press.

Kerr, O. S. (2001, March). Computer Records and the Federal Rules of Evidence. *United States Attorneys' USA Bulletin*, *49*(2). Retrieved on 11th November 2014 from http://www.justice.gov/usao/eousa/foia_reading_room/usab4902.pdf.

Kirby, M. D. (2008). The Urgent Need for Forensic Excellence. *Criminal Law Journal*, *32*.

Kizekova, A. (2012, February 22). The Shanghai Cooperation Organization: challenges in Cyberspace – Analysis. *RSIS Commentaries*, No. 033/2012. Retrieved 11th November 2014 from http://www.eurasiareview.com/27022012-the-shanghai-cooperation-organisation-challenges-in-cyberspace-analysis/.

Koen, R., & Olivier, M. (2008, July). The Use of File Timestamps in Digital Forensics. *ISSA*. Retrieved on 11th November 2014 from http://icsa.cs.up.ac.za/issa/2008/Proceedings/Full/43.pdf.

Kshetri, N. (2010). *Global Cybercrime Industry: Economic, institutional and strategic perspectives*. Berlin Heidelberg: Springer Science & Business Media.

Kshetri, N. (2013). Cybercrime in the Former Soviet Union and Central and Eastern Europe: Current status and key drivers. *Crime Law and Social Change*, *60*(1), 39-65.

Laughner v State, 769 N.E.2d 1147 (Ind. Ct. App. 2002).

Lee, R. (2014, November 19). A triage and collection strategy for time-sensitive investigations. *Guidance Software Webinars*. Retrieved on 19th November 2014 from https://www.guidancesoftware.com/Resources/Pages/webinars/A-Triage-and-Collection-Strategy-for-Time-Sensitive-Investigations.aspx.

Leibolt, G. (2010). The Complex World of Corporate Cyber Forensics Investigations. In J. Bayuk (Ed.), *CyberForensics* (pp. 7-27). New York: Springer Science+Business Media.

Leibrock, L. R. (2008). Duties, Support Functions, and Competencies: Digital Forensics Investigators. In J. J. Barbara (Ed.), *Handbook of Digital and Multimedia Forensic Evidence* (pp. 91-102). Totowa, NJ: Humana Press Inc.

Lempert, R. O., & Saltzburg, S. A. (1983). *A Modern Approach to Evidence*, 2nd edition. St. Paul, MN: West Publishing.

Li, B., Erdin, E., Güneş, M. H., Bebis, G., & Shipley, T. (2011, April 27). An Analysis of Anonymizer Technology Usage. In J. Domingo-Pascual, Y. Shavitt, & S. Uhlig (Eds.), *Traffic Monitoring and Analysis*, Proceedings of the Third COST TMA International Workshop on Traffic Monitoring and Analysis, Vienna, Austria (pp. 108-121). Berlin Heidelberg: Springer.

Li, B., He, J., Huang, J., & Shi, Y. Q. (2011). A survey on image steganography and steganalysis. *Journal of Information Hiding and Multimedia Signal Processing*, *2*(2), 142-172.

Liao, Y. (2001). Analysis of computer crime characteristics. *Journal of Information Technology and Society*, *1*, 119-133.

Lichtblau, E. (2012, March 12). Police Are Using Phone Tracking as a Routine Tool. *The New York Times*. Retrieved on 13th November 2014 from http://www.nytimes/2012/04/01/us/police-tracking-of-cellphones-raises-privacy-fears.html?pagewanted=all&_r=0.

Lidsky, L. B., & Cotter, T. (2007). Authorship, Audiences, and Anonymous Speech. *Notre Dame Law Review*, *82*, 1537-1604.

Lubacz, J., Mazurczyk, W., & Szczypiorski, K. (2010, February). Voice Over IP: The VoIP Steganography Threat. *IEEE Spectrum*. Retrieved on 9th November 2014 from

http://spectrum.ieee.org/telecom/internet/vice-over-ip-the-voip-steganography-threat.

Luen, T. W., & Al-Hawamdeh, S. (2001, October). Knowledge management in the public sector: principles and practices in police work. *Journal of Information Science*, 27(5), 311-318.

Lupsha, P. A. (1996). Transnational Organized Crime Versus the Nation-State. *Transnational Organized Crime*, *2*(1), 21-48.

Lusthaus, J. (2012). Trust in the world of cybercrime. *Global Crime*, *13*(2), 71-94.

Lusthaus, J. (2013). How organised is organised cybercrime? *Global Crime*, *14*(1), 52–60.

Maher, J. (2013, May 5). Loveland's Cyber Crimes Unit grows, but still sees backlog of cases. *Reporter-Herald*. Retrieved on 11th November 2014 from http://www.reporterherald.com/news/loveland-local-news/ci_23174314/lovelands-cyber-crimes-unit-grows-but-still-sees.

Mandel, R. (1987). Distortions in the Intelligence Decision-Making Process. In S. J. Cimbala (Ed.), *Intelligence and Intelligence Policy in a Democratic Society* (pp. 69-83). Transnational Publishers: Hudson, NY.

Marcella Jr, A. J., & Greenfield, R. S. (Eds.) (2002). *Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes*, 2nd edition. CRC Press.

Marshall, A. (2008). *Digital forensics, digital evidence in criminal investigation*. United Kingdom: Wiley-Blackwell.

McAllister, A. (2015, February 4). Ross Ulbricht, in the library, with the laptop: Silk Road boss found guilty of all charges. *The Register*. Retrieved 2nd March 2015 from http://www.theregister.co.uk/2015/02/04/ross_ulbricht_guilty_verdict/.

McGrath, M. G., & Casey, E. (2002). Forensic psychiatry and the Internet: Practical perspectives on sexual predators and obsessional harassers in cyberspace. *Journal of the American Academy of Psychiatry and the Law*, *30*(1), 81-94.

McQuade III, S. C. (2006). *Understanding and Managing Cybercrime*. New York: Pearson Education, Inc.

Middleton, B. (2002). *Cyber Crime Investigator's Field Guide*. London: CRC Press LLC.

Millen, P. (2000, December 8). Under the microscope: a personal view. *Police Review*, 28-29.

Mills, E. (2012, July 2). Cybercrime moves to the cloud. *CNET Australia*. Retrieved on 11th November 2014 from http://www.cnet.com/news/cyber crime-moves-to-the-cloud/.

Mislan, R. P. (2010, June 30). Cellphone crime solvers. *IEEE Spectrum*, 1-3. Retrieved on 7th November 2014 http://spectrum.ieee.org/computing/software/cellphone-crime-solvers.

Mitchell, K. J., Wolak, J., & Finkelhor, D. (2005). Police posing as juveniles online to catch sex offenders: Is it working? *Sex Abuse*, *17*, 241-267.

Mitchell, K. J., Wolak, J., & Finkelhor, D. (2005).The Internet and family and acquaintance sexual abuse. *Child Maltreat*, *10*, 49-60.

Mora, R. J., &Kloet, B. (2010). *Digital Forensic Sampling*. Retrieved on 11th November 2014 from https://blogs.sans.org/computer-forensics/files/2010/03/statisticalforensictriage.pdf.

Morris, S. (2004). The future of netcrime now: Part 1 – threats and challenges. Home Office Online Report 62/04. Retrieved on 26th February 2015 from

http://www.globalinitiative.net/download/cyber crime/europe-russia/Home%20Office%20-%20The%20future%20of%20netcrime%20now%20-%20Part%201%20%E2%80%93%20threats%20and%20challenges.pdf.

Morrissey, S. (2010). *iOS Forensic Analysis: for iPhone, iPad, and iPod touch*. Springer Science+Business Media.

Mutnick, K. D., & Simon, L. W. (2002). *The Art of Deception: Controlling the Human Element of Security*. Indianapolis, Indiana: Wiley Publishing John Wiley & Sons, Inc.

Nakashima E. & Gellman, B. (2015, April 10). As encryption spreads, U.S. grapples with clash between privacy, security. *The Washington Post*. Retrieved June 12th 2015 from http://www.washingtonpost.com/world/national-security/as-encryption-spreads-us-worries-about-access-to-data-for-investigations/2015/04/10/7c1c7518-d401-11e4-a62f-ee745911a4ff_story.html.

Nanji, A. (2005, 10 February). Prosecutors Feel The 'CSI Effect'. *CBS News*. Retrieved on 19th February 2015 from http://www.cbsnews.com/news/prosecutors-feel-the-csi-effect.

National Institute of Standards and Technology (2011, November). US Government Cloud Computing Technology Roadmap Volume II Release 1.0 (Draft): Useful Information for Cloud Adopters. In Draft Special Publication 500-293, United States Department of Commerce, Gaithersburg. Retrieved on 17th October 2014 from http://www.nist.gov/itl/cloud/upload/SP_500_293_volumeII.pdf.

Nelson, B., Phillips, A., & Steuart, C. (2010). Cell Phone and Mobile Device Forensics. In B. Nelson, A. Phillips & C. Steuart (Eds.), *Guide to Computer Forensics and Investigations*, 3rd edition (pp. 495-509). Boston, MA: Course Technology.

Neufeld, P. J., & Colman, N. (1990, May). When Science Takes the Witness Stand, *Scientific American*, *262*(5), 46-53.

Noblett, M. G., Pollitt, M. M., & Presley, L. A. (2000). Recovering and Examining Computer Forensic Evidence. *Forensic Science Communications*, *2*(4). Retrieved on 11th November 2014 from http://www.fbi.gov/about-us/lab/forensic-science-communications/fsc/oct2000/computer.htm.

Nuth, M. S. (2008). Crime and technology – Challenges or solutions? Taking advantage of new technologies: For and against crime. *Computer Law & Security Report*, *24*, 437–446.

O'Connor, V. (2012, March). Common Law and Civil Law Traditions. *International Network to Promote the Rule of Law*. Retrieved on 8th November 2014 from http://inprol.org/sites/default/files/publications/2012/common_law_civil_law_pg_final.pdf.

O'Harrow, R. (2005). *No Place to Hide*. New York: Free Press.

Office of the United Nations High Commissioner for Human Rights (2015, 22 May). Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye. *Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development*. Human Rights Council, Twenty-ninth session, agenda item 3, A/HRC/29/32. Retrieved on June 13th 2015 from http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Documents/A.HRC.29.32_AEV.doc.

Ohio v Roberts, 448 U.S. 56 (1980).

Omnibus Crime Control and Safe Streets Act (1968).
Onyshikiv, Y., & Bondarev, A. (2012, March 8). Ukraine thrives as cyber crime haven. *Kyiv Post*. Retrieved on 9th November 2014 from http://smart-payments.info/eng/publication-one/124.html.
Pallaras, P. (2011). New Technology: opportunities and challenges for prosecutors. *Crime, Law and Social Change*, *54*(1), 71-89.
Parker, J. S., & Kobayashi, B. H. (1999). Evidence. In B. Bouckaert & G. De Geest (Eds.), *Encyclopedia of Law and Economics*, vol. 5 (pp. 290–306). Cheltenham, UK: Edward Elgar.
People v Holowko, 486 N.E.2d 877 (III. 1985).
Perlroth, N. (2015, July 7). Security Experts Oppose Government Access to Encrypted Communication. *The New York Times*. Retrieved on 5th August 2015 from http://nyti.ms/1H739kz.
Phillips, J. H., & Bowen, J. K. (1989). *Forensic Science and the Expert Witness*, revised edition. Sydney: The Law Book Co.
PMSEIC Working Group on Science, Crime Prevention and Law Enforcement (2000, June 2). Science, Crime Prevention and Law Enforcement. Retrieved on 3rd November 2014 from http://www.industry.gov.au/science/PMSEIC/Documents/ScienceCrimePreventionAndLawEnforcement.rtf.
Pocar, F. (2004). Defining Cyber-Crimes in International Legislation. *European Journal on Criminal Policy and Research*, *10*, 27–37.
Poeter, D. (2012, February 28). IBM says it's 'on the cusp' of building a quantum computer. *PC Mag*. Retrieved on 15th June 2015 from http://www.pcmag.com/article2/0,2817,2400930,00.asp.
Ponemon Institute (2015, May 23). 2015 cost of data breach study: Global analysis. *Ponemon Institute Research Report*. Retrieved on 1st June 2015 from http://public.dhe.ibm.com/common/ssi/ecm/se/en/sew03053wwen/SEW03053WWEN.PDF
Post, J. M., Ruby, K. G., & Shaw, E. D. (2000). From Car Bombs to Logic Bombs: The Growing Threat from Information Terrorism. *Terrorism and Political Violence*, *12*, 97–122.
PP v Neo Koon Seng [2008] SGDC 225.
R v Button [2001] QCA 133.
R v Caffrey (Southwark Crown Court, 17 October 2003).
R v Fraser, 2011 BCSC 32.
Raymond, T (2006). The Future for Forensic Scientists. *Australian Journal of Forensic Sciences*, *38*(1), 3-21.
Re VeeVinhnee, Debtor American Express Travel Related Services Company, Inc v VeeVinhnee 336 BR 437 (9th Cir BAP, December 16, 2006).
Regulation of Investigatory Powers Act (2000) (United Kingdom).
Reilly, D., Wren, C., & Berry, T. (2010, November 8-11). Cloud computing: forensic challenges for law enforcement. Paper presented at the *International Conference for Internet Technology and Secured Transactions*, London, UK.
Reilly, D., Wren, C., & Berry, T. (2011, March). Cloud computing: Pros and Cons for Computer Forensic Investigators. *International Journal Multimedia and Image Processing*, *1*(1), 26-34.

Reuters (2015, June 11). Russian hackers accused of attacks on Bundestag and French TV broadcaster. *The Telegraph*. Retrieved on 12th June 2015 from http://www.telegraph.co.uk/news/worldnews/europe/germany/11666815/Russian-hackers-accused-of-Bundestag-attack.html.

Ritter, N. (2006). Digital Evidence: How law enforcement can level the playing field with criminals. *NIJ Journal*, *254*, 20. Retrieved on 13th October 2014 from http://www.nij.gov/journals/254/Pages/digital_evidence.aspx.

Roberts, L. (2008, January). Jurisdictional and definitional concerns with computer-mediated interpersonal crimes: An Analysis on Cyber Stalking. *International Journal of Cyber Criminology*, *2*(2), 271-285.

Robertson, J. (2004). Crime scene investigation: key issues for the future. In J. Horswell (Ed.), *The practice of crime scene investigation* (pp. 389-424). Boca Raton: CRC Press.

Robertson, J. (2012). Forensic science, an enabler or dis-enabler for criminal investigation? *Australian Journal of Forensic Sciences*, *44*(1), 83-91.

Robertson, J., Riley, M., Strohm, C., & Chan, M. (2014, December 10). The year of hacking dangerously - 7 scary cyberattacks. *Bloomberg*. Retrieved on 12th January 2015 from http://www.bloomberg.com/slideshow/2014-12-10/the-year-of-hacking-dangerously.html?#slide1.

Rogers, M. (2011). Digital Crime Scene Analysis (DCSA). *Encyclopedia of Information Assurance* (pp. 855-865). New York: Taylor and Francis.

Rosendale, L. (2012, December 3). A math professor works in digital forensics. *Calvin*. Retrieved March 9th 2015 from http://www.calvin.edu/news/archive/a-math-professor-works-in-digital-forensics

Roth, B. R. (2005, September). State sovereignty, international legality, and moral disagreement. Paper presented at the Annual Meeting of the American Political Science Association. Retrieved on 9th May 2014 from http://www.ihrr.net/files/2006ss%20/State-Sovereignty-Int-Legality-Morality-Roth-2005.pdf.

Saferstein, R. (1983). Forensic Science Winds of Change. In S. M. Gerber (Ed.), *Chemistry in Crime*. New York: American Chemical Society.

Saferstein, R. (1987). *Criminalistics: an introduction to forensic science*. Eaglewood Cliffs, New Jersey: Prentice-Hall, Inc.

Sanett, S. (2000).Authenticity as a requirement of preserving digital data and records. *IASSIST Quarterly*, Spring, 15-18.

Sanger, D. E. & Davis, J. H. (2015, June 10). Hackers may have obtained names of Chinese with ties to U.S. Government. *The New York Times*. Retrieved on 16th June 2015 from http://www.nytimes.com/2015/06/11/world/asia/hackers-may-have-obtained-names-of-chinese-with-ties-to-us-government.html?_r=0.

Savage, C. (2010, September 27). U.S. Tries to Make It Easier to Wiretap the Internet. *The New York Times*. Retrieved on 5th November 2014 from http://www.nytimes.com/2010/09/27/us/27wiretap.html?pagewanted+all&_r=0.

Savona, E. U., & Mignone, M. (2004). The Fox and The Hunters: How IC Technologies Change the Crime Race. *European Journal on Criminal Policy and Research*, *10*, 2-26.

Schaul, K. (2015, April 10). Encryption techniques and access they give. *The Washington Post*. Retrieved June 12th 2015 from

http://apps.washingtonpost.com/g/page/world/encryption-techniques-and-the-access-they-give/1665/.

Schjølberg, S., & Ghernaouti-Hélie, S. (2011, February). *A Global Treaty on Cybersecurity and Cyberspace*, 2nd edition. Retrieved on 12th September 2014 from http://www.cybercrimelaw.net/documents/A_Global_Treaty_on_Cybersecurity_and_Cybercrime,_Second_edition_2011.pdf.

Schmitt, M. N. (Ed.) (2013). *The Tallinn Manual on the international law applicable to cyber warfare*. New York: Cambridge University Press.

Schwartz, K. E. (2009). Criminal Liability for Internet Culprits: The Need for Updated State Laws Covering the Full Spectrum of Cyber Customization. *Washington University Law Review*, *87*, 407-436.

Schweitzer, D. (2003). *Incident response: computer forensics toolkit.* Wiley.

Scientific Working Group on Digital Evidence (SWGDE) (2000). Proposed Standards for the Exchange of Digital Evidence. *Forensic Science Communications*, *2*(2).Retrieved on 11th November 2014 from http://www.fbi.gov/about-us/lab/forensic-science-communications/fsc/april2000/swgde.htm/.

Shafritz, R. (2001). A Survey of Cyberstalking Legislation. *UWLA Law Review*, *32*, 223-338.

Shar, M. Z. (2004, June 24-25). How Lawyers Cross-Examine, Impeach, and Destroy Expert Witnesses. Presentation delivered before the *13th Annual National Expert Witness Conference*, Hyannis, Cape Cod, MA.

Shavers, B. (2013).*Placing the Suspect Behind the Keyboard: Using Digital Forensics and Investigative Techniques to Identify Cyber crime Suspects*. Waltham, MA: Syngress.

Shelley, L. I. (2003). Organized Crime, Terrorism and Cybercrime. In A. Bryden & P. Fluri (Eds.), *Security Sector Reform: Institutions, Society and Good Governance* (pp. 303-312). Baden-Baden: NomosVerlagsgesellschaft.

Shelly, L. (2004, September 27). Organized Crime, Cybercrime and Terrorism. *Computer Crime Research Center*. Retrieved on 19th October 2014 from http://www.crime-research.org/articles/Terrorism_Cyber crime/.

Sheu, C. J. (2007). *Criminology*. Taipei: San Min.

Shipley, T. G., & Reeve, H. R. (2006). Collecting Evidence from a Running Computer: A Technical and Legal Primer for the Justice Community. *SEARCH – The National Consortium for Justice Information and Statistics*. Retrieved on 17th October 2014 from http://www.search.org/files/pdf/CollectEvidenceRunComputer.pdf.

Sieber, U. (2012). *Gutachten des Deutschen Juristentags*. Munich: C H Beck.

Simonite, T. (2014, June 10). Digital summit: Microsoft's quantum search for the "next transistor". *MIT Technology Review*. Retrieved on 15th June 2015 from http://www.technologyreview.com/news/528256/digital-summit-microsofts-quantum-search-for-the-next-transistor/.

Small World News (2012, March). *Guide to safely using satphones*. Version 1.0. Retrieved May 10th 2015 from http://smallworldnews.tv/Guide/Guide_SatPhone_English.pdf.

Smith, R. G. (2004). Impediments to the Successful Investigation of Transnational High Tech Crime. *Trends and Issues in Crime and Criminal Justice*, no. 285, Australian Institute of Criminology. Retrieved on 17th October 2014 from http://www.aic.gov.au/documents/0/7/6/%7B076B58BA-37AE-4673-93FB-9C3150D93D0C%7Dtandi285.pdf.

Snyder, F. (2001).Sites of criminality and sites of governance. *Social & Legal Studies*, *10*, 251–256.

Spence-Diehl, E. (2003). Stalking and Technology: The Double-Edged Sword. *Journal of Technology in Human Services*, *22*(1), 5-18.

Spitzberg, B. H., & Hoobler, G. (2002). Cyberstalking and the technologies of interpersonal terrorism. *New Media & Society*, *4*(1), 71-92.

Spitzberg, B. H., & Cupach, W. R. (2003, July–August).What mad pursuit? Obsessive relational intrusion and stalking related phenomena. *Aggression and Violent Behavior*, *8*(4), 345–375.

Stanford Draft International Convention to Enhance Protection from Cyber Crime and Terrorism (December 1999).

Stanley, S., & Horswell, J. (2004). The education and training of crime scene investigators: an Australian Perspective. In J Horswell (Ed.), *The Practice of Crime Scene Investigation*. Boca Raton: CRC Press.

State v Swinton, 847 A. 2d 921 (Conn. 2004).

Stephenson, P. (2003). A comprehensive approach to digital incident investigation. *Information Security Technical Report*, *8*(2), 42-54.

Steve Jackson Games, Inc. v Secret Service, 816 F. Supp. 432 (W.D. Tex. 1993).

Stimson, E. S. (1936). *Conflict of Criminal Laws*. Chicago: The Foundation Press. Retrieved on 8th November 2014 from http://www.constitution.org/cmt/stimson/con_crim.htm.

Subashini, S., & Kavitha, V. (2011). A Survey on Security Issues in Service Delivery Models of Cloud Computing. *Journal of Network and Computer Applications*, *34*(1), 1-11.

Swire, P. & Ahmad, K. (2012). Encryption and Globalization. *The Columbia Science & Technology Law Review*, *13*, 416 - 418.

Taylor, M., Haggerty, J., Gresty, D., & Lamb, D. (2011, March). Forensic investigation of cloud computing systems. *Network Security*, *2011*(3), 4–10.

Taylor, W. R., Fritsch, E. J., Liederbach, J., & Holt, T. J. (2006). *Digital Crime and Digital Terrorism*, 2nd edition. New Jersey: Prentice Hall.

Teppler, S. T. (2009). Digital Data as Hearsay. *Digital Evidence and Electronic Signature Law Review*, *6*, 14-18.

Tetzlaff-Bemiller, M. J. (2011). Undercover Online: An Extension of Traditional Policing in the United States. *International Journal of Cyber Criminology*, *5*, 813-824.

Thaman, S. C. (2013). Legal Systems: Adversarial and Inquisitorial. *Encyclopedia of Forensic Sciences* (pp. 471-475).

The Draft African Union Convention on the Establishment of a Credible Legal Framework for Cyber Security in Africa (AU Draft 01/09/2012).

Thomas, A. (2006, January 31). The CSI effect, Fact or fiction. *The Yale Law Journal Online*. Retrieved on 13th October 2014 from http://www.yalelawjournal.org/forum/the-csi-effect-fact-or-fiction.

Thompson, C. (2014, May 20). The revolutionary quantum computer that may not be quantum at all. *Wired*. Retrieved on 9th June 2015 from http://www.wired.com/2014/05/quantum-computing/.

Tikk, E. (2011). Ten Rules for Cyber Security. *Survival: Global Politics and Strategy*, *53*(3), 119-132.

Timberg, C. (2014, September 9). Apple will no longer unlock most iPhones, iPads for police, even with search warrants. Retrieved on 15th January 2015 from http://www.washingtonpost.com/business/technology/2014/09/17/2612af58-3ed2-11e4-b03f-de718edeb92f_story.html.

U.S. Department of Justice (2007). Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors. *National Institute of Justice*. Retrieved on 13th February 2015 from http://www.ncjrs.gov/pdffiles1/nij/211314.pdf.

U.S. Department of Justice (2007). Investigations Involving the Internet and Computer Networks. *National Institute of Justice*. Retrieved on 8th January 2014 from https://www.ncjrs.gov/pdffiles1/nij/210798.pdf.

U.S. Department of Justice (2009, August). *Cyberstalking: A New Challenge for Law Enforcement and Industry*. Retrieved on 12th October 2014 from http://www.cyber-rights.org/documents/cyberstalkingreport.htm.

U.S. Department of Justice (2010). A Review of the FBI's Investigations of Certain Domestic Advocacy Groups. *Office of the Inspector General*. Retrieved on 9th November 2014 from http://www.justice.gov/oig/special/s1009r.pdf.

U.S. Department of State (2015, May 18). An open and secure Internet: We must have both. Remarks made by John Kerry, Secretary of State, at *Korea University*, Seoul, South Korea. Retrieved 1st June 2015 from http://www.state.gov/secretary/remarks/2015/05/242553.htm.

U.S. Federal Rules of Evidence (1975).

United Nations (1999, May 12). *United Nations Manual on the Prevention and Control of Computer-Related Crime*. International Review of Criminal Policy - Nos. 43 and 44. Retrieved 26th February 2015 from http://www.uncjin.org/Documents/irpc4344.pdf.

United Nations Convention Against Transnational Organized Crime (2000, GA RES/55/25).

United Nations General Assembly (2011, September 14). Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General. *Developments in the field of information and telecommunications in the context of international security*. Sixty-sixth session, item 93 of the provisional agenda, A/66/359. Retrieved 2nd June 2015 from https://ccdcoe.org/sites/default/files/documents/UN-110912-CodeOfConduct_0.pdf.

United Nations Office on Drugs and Crime (2012). *The use of the Internet for terrorist purposes*. Report prepared in collaboration with the United Nations Counter-Terrorism Implementation Task Force. New York: United Nations. Retrieved on 26th February 2015 from http://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf.

United Nations Office on Drugs and Crime (2013, February). *Comprehensive Study on Cybercrime*. Report prepared for the Open-Ended Intergovernmental Expert Group on Cyber crime. New York: United Nations. Retrieved on 26th February 2015 from https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf.

United State v Bennett, 363 F.3d 947 (9th Cir. 2004).

United States v Catabran, 836 F.2d 453 (9th Cir. 1988).

United States v Cestnik, 36 F.3d 904 (10th Cir. 1994).

United States v Dioguardi 428 F.2d 1033 (2d Cir. 1970).

United States v Duncan, 30 M.J. 1284 (N-M.C.M.R. 1990).
United States v Grant, 967 F.2d 81, 83 (2nd Cir. 1992).
United States v Liebert, 519 F.2d 542 (3d Cir. 1975).
United States v Ross William Ulbricht, 14 Cr 68, (KBF).
United States v Salgado, 250 F.3d 438 (6th Cir. 2001).
United States v Santiago, 534 F.2d 768 (7th Cir. 1976).
United States v Siddiqui, 235 F.3d 1318 (11th Cir. 2000).
United States v Simpson, 152 F.3d 1241 (10th Cir. 1998).
United States v Tank, 200 F.3d 627 (9th Cir. 2000).
United States v Whitaker, 127 F.3d 595 (7th Cir. 1997).
United States v Brown, 482 F.2d 1226 (8th Cir. 1973).
Universal Declaration of Human Rights (1948).
Valli, C., & Hannay, P. (2010, September 16). Geotagging Where Cyberspace Comes to Your Place. *SECAU – Security Research Centre School of Computer and Security Science*. Retrieved on 3rd November 2014 from http://data.openduck.com/wp-posts/2010/07/paper-geotagging/valli-hannay-geotagging.pdf.
Van Brocklin, V. (2014, August 20). Cell phone tracking by police: 2 key court decisions explained. *PoliceOne.com*. Retrieved 11th November 2014 from http://www.policeone.com/police-products/police-technology/articles/7481685-cell-phone-tracking-by-police-2-key-court-decisions-explained.
Vienna Convention on the Law of Treaties (1969).
Vincent, M., & Hart, N. (2011). Law in the Cloud. *Law Society Journal*, *50*, 51-53.
Wade, G. (2011). Computer Crime: Investigations. *Encyclopedia of Information Assurance* (pp. 551-562). Taylor and Francis, New York.
Wadhwa, V. (2015, May 11). Quantum computing is about to overturn cybersecurity's balance of power. *The Washington Post*. Retrieved on 22nd May 2015 from http://www.washingtonpost.com/blogs/innovations/wp/2015/05/11/quantum-computing-is-about-to-overturn-cybersecuritys-balance-of-power/.
Walden, I. (2003). Computer Crime. In C. Reed & J. Angel (Eds.), *Computer Law*, 5th edition (pp. 295-329). London: Oxford University Press.
Walden, I. (2005). Crime and Security in Cyberspace. *Cambridge Review of International Affairs*, *18*(1), 51-68.
Wall, D. S. (2001). Cybercrimes and Criminal Justice. *Criminal Justice Matters*, *46*(1), 36-37.
Wall, D., & Williams, M. (2001). Policing diversity in the digital age: Maintaining order in virtual communities. *Journal of Criminology and Criminal Justice*, 7, 391–415.
Walter, C. (2005, July 25). Kryder's Law. *Scientific American*. Retrieved on 11th November 2014 from http://www.scientificamerican.com/article.cfm?id=kryders-law.
Waltz, E. (1998). *Information Warfare*. Norwood: Artech House.
Warren, M. (2009, October 9). Duty to the Court Sometimes Forgotten. Speech delivered by the Hon. Marilyn Warren AC at the *Judicial Conference of Australia Colloquium*, Melbourne. Retrieved on 19th October 2014 from http://jca.asn.au/wp-content/uploads/2013/11/2009OriginalKeynoteAddress.pdf.
Weil, M. C. (2002). Dynamic Time & Date Stamp Analysis. *International Journal of Digital Evidence*, *1*(2). Retrieved on 15th October 2014 from

http://www.utica.edu/academic/institutes/ecii/publications/articles/A048B1E4-B921-1DA3-EB227EE7F61F2053.pdf.

Wettering, F. L. (2001). The Internet and the Spy Business. *International Journal of Intelligence and Counterintelligence*, *14*(3), 342-365.

White, P. C. (2004). *Crime Scene to Court: The Essentials of Forensic Science*, 2nd edition. Cambridge, UK: Royal Society of Chemistry.

Wilber, D. Q. (2015, May 6). Encrypted Devices Let Criminals Go Dark, U.S. Prosecutor Warns. *Bloomberg*. Retrieved on 10th June 2015 from http://www.bloomberg.com/news/articles/2015-05-06/encrypted-devices-let-criminals-go-dark-u-s-prosecutor-warns.

Willing, R. (2008, May 8). 'CSI Effect' has juries wanting more evidence. *USA Today*. Retrieved on 12th October 2014 from http://usatoday30.usatoday.com/news/nation/2004-08-05-csi-effect_x.htm?loc=.

Wolf, J. B. (2000). War Games Meets the Internet: Chasing 21st Century Cybercriminals With Old Laws and Little Money. *American Journal of Criminal Law*, *25*, 95-117.

Yar, M. (2005). The novelty of `cyber crime': An assessment in light of routine activity theory. *European Journal of Criminology*, *2*, 407–427.

Young, M. (2009, December, 8). From Harmonica Flash Drives to Hidden USB Bracelets. *Trend Hunter Tech*. Retrieved on 26th February 2015 from http://www.trendhunter.com/slideshow/disguised-usb-drives.

Zatyko, K., & Bay, J. (2011, December 14). The digital forensics cyber exchange principle. *Forensic Magazine*. Retrieved on 23rd October 2014 from http://www.forensicmag.com/articles/2011/12/digital-forensics-cyber-exchange-principle.

Zavrsnik, A. (2010). Towards an Overregulated Cyberspace. *Masaryk University Journal of Law & Technology*, *4*(2), 173-190.

Zheng, R., Qin, Y., Huang, Z., & Chen, H. (2003, May 27). Authorship Analysis in Cybercrime Investigation. *Lecture Notes in Computer Science*, *2665*, 59-73.

Zhigang, Y. (2011). Cyber Variants of Traditional Crimes and Criminal Law Responses. *Social Sciences in China*, *32*(1), 66-79.

Zonderman, J. (1999). *Beyond the Crime Lab – The New Science of Investigation*, revised edition. Brisbane: John Wiley & Sons.