E-Evidence and International Jurisdictions:  
Creating Laws for the 21st Century  
Amelia Phillips  
CIS and Computer Science Departments  
Highline Community College, Seattle WA  
aphillip@highline.edu  

Abstract  
This paper explores what laws and procedures a country entering the international cyber arena needs to have in place. Developing nations are creating their e-laws and e-commerce laws to do business in today’s world. They can leapfrog over the existing countries and laws to learn what works and what doesn’t. This paper explores the existing international digital laws and some of the challenges that will be faced as technology advances at its current pace.

1.0. Introduction  
Many countries entering the cyber world have the challenge of creating cyber laws and procedures that conform to their national laws and that also allow them to compete in the virtual business and commerce world.

When creating cyber laws, developing nations must take into account that they will be crossing local and international jurisdictional boundaries. Certain items must be addressed when assembling the laws. Existing international laws and regional laws must be examined to pick the primary ones to address. Every country must deal with email, mobile business and devices, data, ecommerce, Black Berries, and PDAS. Privacy laws vary from country to country. Chain of custody, qualifications of examiners, process and procedure must all be considered.

New challenges are on the horizon. Cloud computing is the latest creation. Recent studies show that computers in cars can be hacked, and soon mobile devices will be able to work in low earth orbit. So where is the jurisdiction? What laws apply? How do you create c-laws and procedures to protect your government, commerce and citizens?  

This paper examines how e-evidence is currently handled in various contexts and how a developing nation might want to address the issues.

2.0. Prevalent cases  
E-mail is now used by corporations worldwide to replace agreements, contracts, negotiations, etc [1]. No one contests that business in today’s world requires email, tweets, blogs and social networks. The question becomes the way the e-evidence is handled and the types of cases being addressed. Losavio et al conducted a survey of attorneys in the state of Kentucky. Table 1 shows a summary of those results [1].

<table>
<thead>
<tr>
<th>Case Type</th>
<th>Civil Cases</th>
<th>Criminal Cases</th>
<th>Domestic Cases</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email</td>
<td>49%</td>
<td>9%</td>
<td>31%</td>
</tr>
<tr>
<td>Websites/Internet</td>
<td>42%</td>
<td>20%</td>
<td>38%</td>
</tr>
</tbody>
</table>

Table 1 – Typical e-evidence by case type  
Civil cases see the largest amount of e-evidence in the form of email followed by domestic cases. While over 50% of the attorneys surveyed stated they did not use Internet history in their cases, those who responded say they used that mode of evidence still weighed heavily on the civil and domestic case side. The importance of email and other e-evidence in conducting day to day business cannot be overstated. While currently criminal cases appear (based on the cited study) to use e-evidence the least, that number will most likely change as the legal system becomes accustomed to using such evidence. White collar crime and online fraud is on the increase and the need for standardization is foremost.

3.0. Privacy laws  
US citizens take the expectation of privacy for granted. This is not true worldwide. The challenge for a digital investigation or e-discovery is the legal acquisition of the data or electronic device. Privacy laws can help or hinder such investigations.

Privilege “according to UK common law … allows a person to refuse to testify on a matter or to
withhold information” [2]. Ricci Ieong lists three privilege items which prevents someone from self incrimination, legal counsel privilege, and statements made “without prejudice”.

Most English speaking countries derive their national laws from British or Dutch common law [3]. For non-common law countries, China and Japan stand out as the two most prominent exceptions. Countries doing significant business with those nations should pay careful attention to these items. Despite all the evidence that can be found, the objective is that the e-evidence can stand up in court and that the examiner can hold up under scrutiny.

Since the majority of cases currently are civil court cases, the question becomes “Was the email done on corporate machines?” Developing countries and companies doing business in those nations need to have privacy laws/procedures in place that address the use of computers in the workplace. In the US, most companies have policies in place and have employees sign agreements which acknowledge computers and email in the workplace belong to the corporation. No warrant or subpoena is necessary for internal investigations. It is also common practice for companies to have their own digital investigations group. An employee can be investigated without their knowledge. If a criminal case emerges during such an investigation, the team stops, calls their legal counsel who notifies the authorities.

Many African nations, South Africa and Namibia specifically, have a different procedure. Because of the history of apartheid, it is written into the Namibian constitution that the employee has to be notified they are under investigation by their company. In addition, the authorities or an outside firm would have to be called in to conduct the investigation – not an employee in another area of the company. This is to ensure that evidence is not tampered with and to ensure the e-evidence is not challenged in court. As more of the sub-Saharan nations come fully online, e-laws must be established to deal with their situation and with the global economy. South Africa is one of the wealthiest and up until recent years, one of the more stable countries in the SADC region. Namibia remains one of the more stable.

Determining what procedures have to be in place and what laws apply is challenging.

4.0. Case law

The law has not been able to keep pace with the rapid change in technology. As a result, case law is the only place one can turn to find guidance or to set precedence.

The Shear report [4] regarding the lawsuit of Munshani v. Signal Lake Venture Fund II shows a case in which the e-evidence determined the outcome of a civil case which became a criminal case of fraud and falsification of evidence. The Munshani case is an excellent example of following the trail of all the e-evidence available. Not only were the .pst files examined, but the network server logs were correlated with the other evidence. In the end, the forensics examiner proved that Munshani had falsified the email claiming Signal Lake Venture Capital had told him to make the bond purchase.

The Munshani case only involved 33 storage devices and other digital evidence. A multi-million/billion dollar case today can encompass over 75 hard drives that need to be imaged and contain terabytes of data. The sheer volume alone makes one tread carefully when evaluating the digital forensics specialist and the e-evidence itself.

A country in the process of creating or updating its e-laws and procedures regarding e-evidence should examine cases such as the Munshani case. The Shear report is thorough in its approach by specifying the exact items that were inconsistent and making it easy for the non-technical person to understand. The critical item on a country’s list should be to examine the e-laws and relevant cases of countries they intend to do business with. This will be a determining force in their decision making.

The courts must also be willing and able to enforce and interpret the law. In the case of Steagald v. United States, a Fire Marshall charged that his fourth amendment rights were violated when a warrant was issued to examine his work machine [5]. The Fifth Circuit court ruled in the supervisor’s favor of probable cause because of the suspicions aroused due to child porn newsgroups on the computer. Over 100 files related to child pornography were found on his machine and on zip disks.

The case of Smyth v. Pillsbury was one in which Smyth, an employee, sent inflammatory emails regarding management. He charged that Pillsbury violated his privacy by examining his company email. The court ruled that an employee has no expectation of privacy on the company network and that they were in their rights [6].

Case law for criminal and domestic cases is not readily available at the writing of this paper. As more child custody cases, domestic violence/ harassment and criminal cases are determined with e-evidence, the more that will come into the public view and a matter of public record for review.

Conflicting case law will be the biggest challenge in this arena as the century moves forward.
5.0. The digital forensic specialist

The qualifications of the person examining the evidence should be easily identifiable in all parts of the world. On the international front, many use vendor certifications. The US is currently struggling between what is needed. Several states against the resolution of the American Bar Association (ABA) instituted requirements that all computer forensics investigators be licensed private investigators.

This has resulted in cases coming to a halt until the companies were able to obtain licensing or move their company under a law firm. Michigan amended their law to allow someone with an appropriate higher education degree or recognized computer forensic certification to conduct such investigations [7].

In the US, the question has come down to “is it a state or federal matter to qualify digital investigators?” As we move deeper and deeper into the global economy and as the criminal element reaches its hands across the span of the globe, an international standard is needed that is beyond the boundaries of vendor certification. Various groups such as the ISFCE insert citation here have created certifications which are accepted in many countries. SANS has created a body of knowledge that constitutes what is needed for a person qualified in the field.

The conclusion reached by Phillips and Nance [6] was

The desired characteristics of a computer forensics examiner include 1) competency and 2) credentials that will stand up in a court of law. Perhaps instead of reinventing the wheel, a solution would be to agree upon the body of knowledge and put forth that a court can accept a person who has been certified by a variety of methods.

Since many cases are going to require the cooperation of experts from many fields and many countries, the standards should be agreed upon as to what is needed to be a computer forensics expert. Developing nations should be sure that their National Forensic Science Institute or equivalent has the personnel qualifications in place for such investigations.

6.0. Technology and E-evidence

The ever changing landscape of technology is offering built in solutions and built in challenges for the computer forensics professional. In this section examines these challenges and solutions.

6.1. Email evidence

As stated earlier, email evidence is taking the place of negotiations, contracts and other legal documents. How this e-evidence is handled is critical in today’s global environment. The Munshani vs. Signal Lake case shows how such an investigation should be handled with corroborating evidence from not only the various alleged recipients of said email, but the email server itself.

Global companies are facing this issue on a grand scale. The case involving Michael Sears, the former CFO of Boeing, and Darlene Druyun of the Air Force required extensive combing of email evidence to determine who was or was not involved in the contract negotiations [8]. If the case involved employees who were physically in other countries, different procedures had to followed to acquire their drives.

The challenge that is being faced now regarding email is location of the evidence. People can send email from:

- Their corporate computer
- Home computer
- Laptop
- Personal Cell phone
- Corporate Cell phone
- Black Berry
- Unsecured public WiFi
- Secured public WiFi
- VPN

The list will continue to grow as the technology expands and changes. Whose server are things located on? How was it transmitted?

When is a wiretap law needed? When are you dealing with stored messages? The challenge with many mobile devices is they change monthly as the technology progresses and each vendor is trying to outsmart the other with the capabilities. How to put laws in place that addresses these issues is another challenge.

There have been agreements in place for many years for how the various vendors deal with subpoenas and warrants. As recently as ten years ago, AOL kept customer emails for up to 90 days. Now you are lucky as an investigator if you can get two weeks because of the sheer increase in volume.

The challenge will only increase as the use of digital devices continues to permeate almost every aspect of people’s lives.
6.2. Virtual machines

Virtual machines make training and dealing with legacy software much easier. Microsoft itself has created an XP mode for Windows 7. When reading the instructions, a user has to download and install Virtual PC and then install XP. It is simply a virtual machine.

Investigating virtual machines is straightforward, but actually verifying that one has been on the machine to begin with is not always easy. VMs fit on flashdrives that easily go into someone’s pocket. Virtual desktops are becoming standard in many computer labs. What evidence is going to be left behind by those? How will they be used by the criminal element or even corporate spies?

6.3. Cloud computing

Cloud computing is getting press everywhere. The challenge is that no one can accurately describe “the cloud” and all its implications. There are currently three different types of clouds that are deployed. Each has its own pros and cons.

Dan Morrill states that cloud computing such as the one employed by Amazon will make computer forensics easier [9]. When presented with a “preservation letter” a company or their agent can easily backup the environment and store it for later examination. Also the system automatically hashes all files.

While that makes certain parts of the forensic examination of cloud computing “forensic friendly”, the question remains as to chain of custody. Where physically is that part of the cloud at any given time? And where was it when forensically acquired? And while it may prove to be very easy and straightforward as a direct result of the design, policies and procedures need to be in place to handle it. And country developing e-laws needs to take a close look at what is happening in the cloud arena and how it affects their government, their companies and their citizens.

7.0. Jurisdiction and the courts

Mobile devices and the cloud are turning acquisition and chain of custody into a jurisdictional challenge. Do we apply the laws the way tax laws are applied? For example, if someone in South Africa has an ecommerce host in Germany (or other EU country) for their company, they pay taxes to Germany. So if the person’s mobile device is used to transmit sensitive or fraudulent information are they subject to the country in which they are caught or their country of origin or the country where their mobile device is serviced?

The Cybercrime Convention of 2001 compiled a treaty regarding many of these issues. Rustad offers a summary of the most pertinent ones that any country coming into the global economy needs to pay heed to [10]:

- Articles 2-4 asks “signatory states” to create national laws regarding computer crimes
- Article 5 criminalizes transmission of malware
- Articles 7 and 8 address “computer related forgery and fraud”
- Article 9 criminalizes distribution of child pornography
- Articles 10 and 11 address aiding and abetting computer crimes
- Article 17 makes computer crimes an extraditable offense

In March of 2010, some legislators asked President Obama to put “some teeth” [11] into a cyber crime bill to prevent “cyber crime havens”. While this may be a good start, what is actually needed is proper education of developing nations as to what can be done in the global cyber community and help them establish their e-laws and procedures of dealing with e-evidence.

At the start of the paper, the idea of communication in low earth orbit was mentioned. The reality of that is within the next few years. Privatization of the US space program along with other nations going to the moon means people will be “phoning home” from outer space.

Whose jurisdiction is it? Does there need to be an international court for these crimes? Where are we headed in the next 10, 20, 30 or 50 years?

8.0. Conclusions

Developing nations and even those currently online need laws in place to deal with evolving technology and design them in such a way that the laws can be easily adapted and applied to technology that does not yet exist. Today we see the challenge presented by cloud computing. As new devices and techniques are created, there is a promise of even more.

Cybercrime and the investigation of it is not going away. And as our world becomes more and more connected in the digital age, the structure needs to be put into place that can handle and grow with it. Cooperation between nation states needs to be
cultivated so that the “cyber crime havens” do not have a place to take hold. The differences between English speaking based and non-English speaking based countries need to be addressed. A thorough examination of extradition treaties and understanding of how they affect cyber crime law enforcement is something that has not been conducted or quantified.

The challenges presented in this paper need to be dealt with by international cyber community and by each nation.

9.0. References


