2015

Attribution Evidence of Cell Phone Data

Sana Haider

Case Western Reserve University

School of Law

Memorandum for the Office of the Prosecutor

Special Tribunal For Lebanon

Issue: Attribution Evidence of Cell Phone Data

Prepared by:
Sana Haider
J.D. Candidate 2015
Spring 2015

Table of Contents	**Page**
1. Introduction	8
A. Scope	8
B. Summary of Conclusions	8
i. Attribution evidence falls in different categories criminal proceedings depending on the domestic court.	8
ii. In the United States, attribution evidence is usually an issue controlled by the fourth amendment.	8
iii. In the UK, the question of the attribution evidence is also inconclusive based on court rulings.	9
iv. Most domestic courts do not have one specific test for attribution evidence in courts.	9
v. In determining whether to "attribution evidence" is admitted, the Special Tribunal For Lebanon should follow a two-step process.	10
II. Factual Background	10
III. Legal Discussion	12
A. The proper use and scope of the search warrant determines the admission of cell phone evidence in the U.S.	12
i. Warrantless Searches do not usually allow for admission of cell/mobile phone and digital data in court.	14
ii. The burden of proof is determined the scope of the warrant the legality of the search.	16
iii. Courts can apply Federal Rules of Evidence to attribute the evidence	17

to the person.	
B. Search warrants and restrictions of preliminary to admission of digital data as evidence in the UK.	20
C. Digital data standards for forensic use varies within domestic courts.	24
IV. Conclusion	25

Bibliography of Sources:

Special Tribunal for Lebanon and Lebanese Law:

1. Code of Professional Conduct for Defence Counsel and Legal Representatives of Victims appearing before the Special Tribunal for Lebanon. Special Tribunal For Lebanon. Adopted December 14, 2012. Located at www.stl-tsl.org/index.php?option=com_k2&Itemid=291&id=2097_7644ccab3246f3883847f693e56657f2&lang=en&task=download&view=item

2. *Lebanese Code of Criminal Procedure. STL Draft Official Translation from Arabic.* https://www.stl-tsl.org/index.php?option=com_k2&Itemid=421&id=3240_08b8455a66e7745ce40c54baa52e1c75&lang=en&task=download&view=item

3. Special Tribunal for Lebanon. About the STL. Located at http://www.stl-tsl.org/en/about-the-stl.

4. Interlocutory Decision on the Applicable Law: Terrorism, Conspiracy, Homicide, Perpetration, Cumulative Charging. STL-11-01/I/AC/R176bis

5. Memorandum of understanding between the Government of the Republic of Lebanon and the Special Tribunal for Lebanon concerning the office of the Special Tribunal of Lebanon. Located at www.stl-tsl.org/index.php?option=com_k2&Itemid=286&id=146_79897eb2918796ab6c5c4259e8e1e06a&lang=en&task=download&view=item

6. Rules of Evidence and Procedure. Special Tribunal for Lebanon. Amended February 12, 2015. Located at www.stl-tsl.org/images/RPE/RPE_EN_February_2015.pdf

7. Special Tribunal for Lebanon Casebook. Major Rulings issued by the Special Tribunal. 2012. Located at http://www.stl-tsl.org/index.php?option=com_k2&Itemid=1063&id=4536_e97d2efe7d315853da30cb41b9e6711f&lang=en&task=download&view=item

8. Statute of the Special Tribunal for Lebanon. S/RES/1757 (2007). [Security Council Resolution 1757].

US Law/Statutes

9. USCS Fed Rules Evid. R 901

10. USCS Fed Rules Evid. R 902

11. USCS Fed Rules Evid. R 702

12. USC. Amendment 4. Search and Seizure.

US Cases:

13. Brown v. State, 767 S.E.2d 299 (Ga. Ct. App. 2014).

14. Chimel v. Cal., 395 U.S. 752, 89 S.Ct. 2034 (1969).

15. In re Search of Apple iPhone, 31 F. Supp. 3d 159 (D.D.C. 2014).

16. Linde v. Arab Bank. 922 F. Supp.2d 316 (2013) US. District Court. E.D. NY.

17. New York v. Belton, 453 U.S. 454, 101 S. Ct. 2860, 69 L. Ed. 2d 768 (1981).

18. Rakas v. Illinois, 439 U.S. 128, 130-31 n.1, 58 L. Ed. 2d 387, 99 S. Ct. 421 (1978)

19. Riley v. California, 134 S.Ct. 2473 (2014)

20. Roberts v. Howton, 13 F. Supp. 3d 1077 (D. Or. 2014).

21. State v. Davis, 13-275 (La. App. 3 Cir 10/23/13), 129 So. 3d 554

22. Tackett v. United States, 2014 U.S. Dist. LEXIS 170845 (S.D. Ohio Nov. 21, 2014)

23. Terry v. Ohio, 392 U.S. 1, 88 S.Ct. 1868 (1968).

24. U.S. v. Curry, 2008 WL 219966 (D. Me. 2008).

25. United States v. Gholston, 993 F. Supp. 2d 704 (E.D. Mich. 2014)

26. US v. Mejia. 545 F. 3d 179 - Court of Appeals, 2nd Circuit, 2008.

27. United States v. Wurie, 728 F.3d 1 (1st Cir. 2013)

UK

28. ACPO Good Practice Guide for Digital Evidence. Association of Chief Police Officers. (Adopted by Police Forces in England, Wales, and Northern Ireland. 2012. Located at http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=4&ved=0CDEQFjAD&url=http%3A%2F%2Fwww.digital-detective.net%2Fdigital-forensics-documents%2FACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf&ei=4PUrVfK3E4TfsASIp4HADg&usg=AFQjCNFC7xajX8s_4yk5Sif9MvalLf4hig&sig2=8HPhKoYW6W0mjVZj47DmTg&bvm=bv.90491159,d.cWc&cad=rja

29. Civil Evidence Act of 1995. Located at http://www.legislation.gov.uk/ukpga/1995/38/contents

30. Data Protection Act of 1998. Located at https://www.gov.uk/data-protection/the-data-protection-act

31. Russel Knaggs and Ramzy Khachik v. United Kingdom-46559/06 [2011] ECHR 1328. European Court of Human Rights. August 2011.

32. Suleman v. R[2012] [2012] 2 Cr App R 30, [2012] EWCA Crim 1569

33. Terrorism Act of 2000. Located at http://www.legislation.gov.uk/ukpga/2000/11/contents

34. [2012] 3 WLR 515, [2013] QB 1, [2012] EWCA Crim 2, [2012] Crim LR 539, [2012] 2 All ER 947, [2012] 1 Cr App R 26 (17 January 2012). *Located at http://www.bailii.org/ew/cases/EWCA/Crim/2012/2.html*

Books, Websites, and Articles:

35. Afentis Forensics. http://afentis.com/expert-witness/about/

36. Adam M. Gershowitz. *Seizing a Cell Phone Incident to Arrest: Data Extraction Devices, Faraday Bags, or Aluminum Foil as a Solution to the Warrantless Cell Phone Search Problem. William & Mary Bill of Rights, Vol. 22, 2014, Forthcoming William & Mary Law School Research Paper No. 09-252. August 21, 2013.*

37. Alamuddin, Amal, Jurdi, Nidal Nabil, and Tolbert, David. The Special Tribunal for Lebanon Law and Practice. GB Oxford UK. 2004.

38. Ed Markey United States Senator for Massachusetts Report. For Second Year in a Row, Markey Investigation Reveals More Than One Million Requests By Law Enforcement for Americans Mobile Phone Data. December 9, 2013. Located at http://www.markey.senate.gov/news/press-releases/for-second-year-in-a-row-markey-investigation-reveals-more-than-one-million-requests-by-law-enforcement-for-americans-mobile-phone-data

39. How Digital Rights Ireland Litigated against EU Data retention and Won. Electronic Freedom Frontier. 2014. Located at https://www.eff.org/node/81899.

40. Jordan J. Paust. Panel: Cybercrimes and the Domestication of International Criminal Law. University of Houston Law Center. June 12, 2014. *5 Santa Clara Journal of International Law 2 (2007)*

41. Lucy L. Thompson. Mobile Devices: New Challenges for admission of Electronic Devices. SciTech Lawyer Vol. 9. American Bar Association. Winter/Spring 2013.

42. ESSAY: Untangling Attribution, 2 Harv. Nat'l Sec. J. 531, 532

43. Project on Tor. https://www.torproject.org/

I. Introduction

A. Scope

In this paper I will present the methods of dealing with attribution evidence in domestic courts, focusing on the United States, the UK, and the European Commission as well as the standards for evidence set forth by the Special Tribunal for Lebanon (the "STL"). This article will look at the process by which a user of a device, such as a computer or a telephone, is identified through the consideration of other evidence, such as contacts profiles for mobile telephones, content of messages such as SMS (text messages) or emails, geographic location of the device in question, co-location with other mobile phones or digital devices. Article I also focuses on whether attribution is a pre-cursor to admitting particular digital evidence. Domestic Courts differ on what evidence should be considered by courts when considering whether a cell phone or computer or other device may be attributed to a particular individual. Please note that while various countries and cases use the term "cell phone" and "mobile phone" interchangeably, I will be using the term "cell phone" in this paper.

B. Summary of Conclusions

i. Attribution evidence falls in different categories of criminal proceedings depending on the domestic court.

In most cases, the court determines how the evidence was obtained, the scope of the search they may do with the evidence, and the relevance of the evidence to the crime.

ii. In the United States, attribution evidence is usually an issue controlled

by the fourth amendment[1].

The scope of the warrant often controls how that evidence can be used. Federal Rules of Evidence allow admission of digital data with restrictions. Although digital data often has to be authenticated, this authentication does not necessarily mean it must be attributed to the suspected person to be used as evidence in court.

iii. In the UK, the question of the attribution evidence is also inconclusive based on court rulings.

The judge usually determines whether the evidence is admissible to be used. Often, if the judge thinks the evidence is relevant to the case, he allows these facts to be presented to the criminal trial. The evidence must still be legally obtained.

iv. Most domestic courts do not have one specific test for attribution evidence in courts.

Generally, the evidence must satisfy core requirements such as: relevance to the accused

---

* This topic will require comparative law research on domestic practice. The OTP is interested in the treatment of "attribution evidence" in domestic courts. By attribution, we mean the process by which a user of a device, such as a computer or a telephone, is identified through the consideration of other evidence, such as contacts profiles for mobile telephones, content of messages such as SMS (text messages) or emails, geographic location of the device in question, co-location with other mobile phones or digital devices. (In our case, the OTP is interested in attribution of mobile telephones, but examples of courts considering evidence to identify the user of other devices, such as the user of a personal computer, would also be relevant.) The research should address what evidence has been considered by courts when considering whether a mobile phone or computer or other device may be attributed to a particular individual. Have courts established particular standards for considering whether a mobile telephone or other device may be attributed to an individual user? Is attribution a pre-cursor to admitting particular digital evidence, for example, if the case involves calls made on a mobile phone, will a court first determine whether it believes that mobile phone can be attributed to an accused before admitting the relevant evidence related to that phone? Have courts favored particular kinds of evidence when considering attribution? Have courts required that any such evidence be admitted through witness testimony? Or are there also examples of the evidence being admitted upon the request of a party?

[1]USC. Amendment 4. Search and Seizure. [Reproduced in the accompanying CD at Source 12]

crime, admissibility of the search, scope of the digital data search, and other surveillance or forensic ties that corroborate the suspect to the digital data of the device in question. Attribution is usually divided into device attribution: did the cell phone or computer in question transmit the messages or data, and human attribution: did the suspect actually transmit or use the device. Forensic evidence for the technical attribution is much easier to obtain than human attribution.

v. In determining whether "attribution evidence" is admitted, the Special Tribunal For Lebanon should follow a two-step process:

a. The Office of the Prosecutor should make sure it has a warrant or legal permission of invasion or search of the suspect. Even if proper forensic procedures are followed to show that the suspect actually used the device for the incriminating data, the attribution evidence will not be accepted without a valid warrant for the contents on the device.

b. The Office of the Prosecutor should create and use a standard forensic attribution model that it uses as a guideline to link digital data to users and owners. This model should be consistent with accepted scientific forensics.

II. Factual Background

The Special Tribunal for Lebanon has a focused goal of finding and prosecuting the terrorists responsible for the February 2005 attack in Lebanon. The Tribunal does not currently have a set standard for the treatment of "attribution evidence" that is the attribution

of digital data from cell phones to specific users. The Rules of Procedure and Evidence for the Special Tribunal in Lebanon allow the prosecution to seize physical evidence of the accused under Rule 62(ii) in cases of urgency[2]. The prosecution then has the responsibility to store and preserve this evidence[3]. In the case of cell phone data and computer data, this preservation can become problematic, especially if online storage devices can be remotely erased causing sensitive and pertinent data linking the suspect to the data to be lost. Countries like the U.S. and UK have a very involved, still developing, system for the legal search, seizure, preservation, and use of digital data.

The Appeals Chamber of the STL gave its opinion outstanding pre-trial legal issues regarding the STL statute in a February 16, 2011 interlocutory decision. In this judgement, the Chamber ruled that "when there is no conflict between Lebanese and international law, the Appeals Chamber states that Lebanese law must be applied. If there is conflict, then the legal system that proves more favourable to the accused must be applied.[4]" There is no clear answer about how to treat digital evidence in international law or the Lebanese Criminal Code, the more favorable solution for the accused is to require a proper warrant.

There are two aspects of attribution, both of which have a different legal issues. First, the messages or data must be linked to a certain device. Second, the messages or data must be linked to a person or persons. In the U.S. both of these issues are warrant-based Fourth Amendment issues. If the warrant is proper it is assumed the data on the device belongs to the

---

[2] Rule 62(ii). Rules of Evidence and Procedure. Special Tribunal for Lebanon. Amended February 12, 2015. www.stl-tsl.org/images/RPE/RPE_EN_February_2015.pdf [Reproduced in the accompanying CD at Source 6]

[3] *Id.*

[4] Interlocutory Decision on the Applicable Law: Terrorism, Conspiracy, Homicide, Perpetration, Cumulative Charging. STL-11-01/I/AC/R176bis [Reproduced in the accompanying CD at Source 4]

person on whom the device was found or the domicile dweller of the home searched[5]. The linking of the attribution of evidence to the natural person associated with this evidence is inferred by the warrant.[6] The Tribunal may be functioning in a different manner than other domestic courts, by first gathering the evidence, then trying to attribute it to a person or persons which upsets the warrant requirements. In the domestic courts, the legal standard is applied to the gathering-of-information stage with warrants.

Currently, the Special Tribunal for Lebanon states that it "may summon and interview witnesses or request the competent authorities of a State to do so, to seize probative materials or to search premises.[7]" There is no clear limit on how theses searches should be performed or the extent to how much or which evidence may be gathered during the searches.

III. Legal Discussion

A. The proper use and scope of the search warrant determines the admission of cell phone evidence in the US.

Under U.S. law, the first step to determining whether a court can use digital data often boils down to whether the evidence was obtained legally. This is a Fourth Amendment issue, focusing on legal search and seizure of individuals and their property.[8] The level of the search is limited by the terms of the scope of the warrant or the scope of the search.

Attribution evidence in searches is defined in the Supreme Court case United States v.

[5] United States v. Gholston, 993 F. Supp. 2d 704 (E.D. Mich. 2014) [Reproduced in the accompanying CD at Source 25]

[6] United States v. Wurie, 728 F.3d 1 (1st Cir. 2013) [Reproduced in the accompanying CD at Source 27]

[7] Rule 92. Rules of Evidence and Procedure. Special Tribunal for Lebanon. Amended February 12, 2015. www.stl-tsl.org/images/RPE/RPE_EN_February_2015.pdf [Reproduced in the accompanying CD at Source 6]

[8] USC. Amendment 4. Search and Seizure [Reproduced in the accompanying CD at Source 12]

Gholston .[9] In *Gholston,* the "attribution" evidence typically found on a cell phone, indicates who has used or controlled the device, and is analogous to the "indicia of occupancy."[10] The concept of searching a phone is similar to searching a dwelling or similar occupancy. This means that the same restrictions that limit the government from searching a dwelling limit it from searching a phone. Following this legal argument, the government needs a warrant that uses the same strict standards to search the cell phone of suspects as it does their homes.

Obtaining a warrant to search the contents of a cell phone still does not necessarily guarantee admissibility of cell phone data as evidence. The court may deem a warrant that simply requests general or all data from a cell phone or computer insufficient. Warrants to search cell phone data must be specific as to the data the state is looking for and the area in which the state expects to find the data, as determined in the case In re Search of Apple iPhone.[11] Searching the contents of the entire phone is usually too broad of a scope for a warrant. In the *Search of Apple iPhone,* the court followed the standard set out in Gholston for the "indicia of occupancy" of the cell phone. In this case, the court argued that because searching the contents of a cell phone was a Fourth Amendment search, the prosecution needed to have a warrant with the proper scope to search.[12] Even though the prosecution had a warrant, it was not specific enough to apply. The government must say in the search warrant what it intends to do with the information it takes. Here, the government search warrant was not descriptive enough about the "forensic evidence"

---

[9] United States v. Gholston, 993 F. Supp. 2d 704 (E.D. Mich. 2014) [Reproduced in the accompanying CD at Source 25]

[10] *Id.*

[11] In re Search of Apple iPhone, 31 F. Supp. 3d 159 (D.D.C. 2014) [Reproduced in the accompanying CD at Source 15]

[12] *Id.*

of the warrant.[13] The standards for a warrant with proper scope vary across districts but the safest method of ensuring admittance of evidence is to have a specific and detailed warrant that not only focuses on the digital content, but also indicates where in the phone data one would reasonably find that content. If the Special Tribunal wants to follow the U.S. method of attributing cell phone evidence, the office of the prosecutor should focus on first having a proper warrant to search the contents of the phone; part of the requirements for that warrant would be to link the suspect or defendant as the user of the phone..

i. Warrantless searches do not usually allow for admission of cell phone and digital data in court.

Warrantless searches are permitted under exigent circumstances and Terry stops. The standard for stop and search is a "reasonable articulable suspicion" under Terry v. Ohio.[14] This allows for a search of the person who the government has a reasonable articulable suspicion poses a danger.[15] Cell phones call logs and digital data stored on the phone are not subject to information that can be obtained as part of the Terry stop or Terry seizure.[16] In Brown v. State, the court ruled against warrantless search of cell phones.[17] In *Brown*, the court ruled that the state must show exigent circumstances for a warrantless search of cell phones; other warrantless

---

[13] *Id.*

[14] Terry v. Ohio, 392 U.S. 1, 88 S.Ct. 1868 (1968). [Reproduced in the accompanying CD at Source 23]

[15] *Id.*

[16] United States v. Wurie, 728 F.3d 1 (1st Cir. 2013). [Reproduced in the accompanying CD at Source 27]

[17] Brown v. State, 767 S.E.2d 299 (Ga. Ct. App. 2014). [Reproduced in the accompanying CD at Source]

searches are considered illegal.[18] While some of the court decisions are split, allowing for limited warrantless searches for incidents to arrest (where the search is a precursor to a later arrest), the overall direction of the courts does not allow warrantless searches of cell phones. Even if evidence from the phones is useful to the prosecution to show evidence of a crime, the court generally requires a warrant for cell phone evidence.

Warrantless car searches or search incidents to arrest also prompt the court to discard cell phone information obtained from these searches. This cell phone protection against warrantless searches was cemented in the Supreme Court case Riley v. California, where the Court ruled that searching the contents of a person's cell phone after arrest without a warrant went beyond the police's right to search-incident-after-arrest[19]. Cell phones are not easily accessible evidence that can easily be used as a weapon or quickly disposed of like drugs. The police or government agents can search a person they arrest[20] but this search does not extend to an extensive search of devices like cell phones or data stored on these devices. In a recent case, U.S. v. Wurie,[21] the Supreme Court also ruled against allowing evidence from cell phones to be used as evidence in court. This case involves an incident from 2007, when Wurie, the suspect, was arrested and tangible data from his flip phone was used to connect him to drug dealing crimes. The court only ruled on this case in 2013[22] While the principle standard of not searching phones after arrest was

---

[18] Riley v. California, 134 S.Ct. 2473 (2014). [Reproduced in the accompanying CD at Source 19]

[19] *Id.*

[20] Chimel v. Cal., 395 U.S. 752, 89 S.Ct. 2034 (1969). [Reproduced in the accompanying CD at Source 14]

[21] United States v. Wurie, 728 F.3d 1 (1st Cir. 2013). [Reproduced in the accompanying CD at Source 27]

[22] *Id.*

the same, since the case started in 2007, cell phones, online and personal data stored on smart [cell] phones had changed exponentially. Cell phone data, tangible and intangible, is reinvented and expanded so quickly, that while the courts may not have a specific standard for determining the scope of the warrant, the recent court decisions show that courts still want some type of standard requiring a warrant.

ii. The burden of proof is determined the scope of the warrant and the legality of the search.

Once the evidence [digital data] is collected, the Supreme Court has ruled that the defendant has the burden of proving that he or she has standing to challenge the legality of the evidence[23]. In U.S. v. Curry, the defendant disclaimed ownership of the phone found in the search.[24] The defendant in Curry had standing to disclaim the contents of the phone because his disclaimer of the phone's ownership postdated the government's search of the phone's contents and data.[25] The defendant often bears the burden of proving the illegality of the search (i.e. that the search warrant was invalid or that there was not search warrant). If the defendant does not raise this claim, then there is nothing that would bar admission of the evidence. In the Special Tribunal for Lebanon, many of the cases are *in absentia*.[26] While the lawyers may still be able to challenge improperly collected evidence, and the defendant may have standing to disclaim the

---

[23] Rakas v. Illinois, 439 U.S. 128, 130-31 n.1, 58 L. Ed. 2d 387, 99 S. Ct. 421 (1978). [Reproduced in the accompanying CD at Source 18]

[24] U.S. v. Curry, 2008 WL 219966 (D. Me. 2008). [Reproduced in the accompanying CD at Source 24]

[25] *Id.*

[26] Alamuddin, Amal, Jurdi, Nidal Nabil, and Tolbert, David. The Special Tribunal for Lebanon Law. [Reproduced in the accompanying CD at Source 24]
and Practice. GB Oxford UK. 114-117. 2004. [Reproduced in the accompanying CD at Source 37]

evidence, if the defendant is not present he cannot disclaim properly.

iii. Courts can apply Federal Rules of Evidence to attribute the evidence to the person.

As mentioned in Part A of this paper, the easiest way of ensuring that cell phone data is admitted in court would be to specify the cell phone content the prosecutor wishes to use in the initial warrant. If this is not possible for some reason, evidence can still be admitted using the Federal Rules of Evidence. Under the criteria set forth by Fed. R. Evid. 702,[27] the prosecution could submit expert witnesses who explain how technical attribution works and give their reasoning for why the cell phones have transmitted data. The standard set out in Fed. R. Evid. 702 that governs testimony submitted by an expert witness is:

> A witness who is qualified as an expert by knowledge, skill, experience, training, or education may testify in the form of an opinion or otherwise if:
>
> - (a) the expert's scientific, technical, or other specialized knowledge will help the trier of fact to understand the evidence or to determine a fact in issue;
> - (b) the testimony is based on sufficient facts or data;
> - (c) the testimony is the product of reliable principles and methods; and
> - (d) the expert has reliably applied the principles and methods to the facts of the case.[28]

For example, an expert witness can explain and testify to the court how cell phone cell sites work and explain why the phone has to have been in a certain geographic location based on cell tower location or phone GPS. The expert witness could also attribute the human source to the data and explain why it is

[27] USCS Fed Rules Evid R 702. [Reproduced in the accompanying CD at Source 9]

[28] *Id.*

likely a certain person can be linked to the data based on forensic evidence and perhaps supplemented by other verifying evidence (like video footage showing the suspect in the spot where the cell phone GPS tracking links the cell phone to be at a certain time). In State v. Davis, an expert in cell site analysis was called to testify about information that the prosecution brought against the witness using her cell phone "pinging."[29] The prosecution wanted to use the cell phone pinging during a phone call she made to show that the suspect was not in the area in which she testified she was during that time. The expert witness explained:

> "that when a phone is in idle mode, it is constantly 'stacking and racking' - meaning '[i]t's taking all the various cell sites that the phone can see and has stacked and racked at the top the one it sees with the clearest signal, the best quality of signal… [The expert witness] prepared a power-point presentation to demonstrate the cell towers used as well as the range of the towers."[30]

While the testimony of the expert witness was thorough and his experiment repeatable, he was working with very little personal data from the suspects cell phone. By using her cell phone and the cell phone towers records, he was able to show that the call she made pinged from a different location than that in which she claimed to be at the time. The court may still require a warrant for the collection of more invasive digital data the expert witness may need to make his analysis. While using expert witness testimony may seem like an extreme standard for admitting evidence, it is the more conservative route. This standard also has the benefit of having a more quantifiable or fact verifiable basis. Cell phone forensic science and attribution is evolving must faster than the courts can address them. Expert witnesses have the benefit of already having Fed. R. Evid. 702 standards that they must meet before they can present their testimony to the jury.

---

[29] State v. Davis, 13-275 (La. App. 3 Cir 10/23/13), 129 So. 3d 554. [Reproduced in the accompanying CD at Source 21]

[30] *Id.*

In State v. Davis, the court allowed evidence presented by the expert witness to show that the suspect's cell phone was not in the location she claimed as in her testimony[31] as impeachment testimony. If the suspect had not wrongly admitted where she was at the questioned time, the cell phone evidence might not have been able to be used in the court by the expert witness as impeachment testimony. In this case, the digital evidence was admissible not only because of the expert witness testimony but because the data was used to impeach the witness. Here the cell phone data collected was fairly minimal and could be verified through a third party source, the cell phone tower data. The Court would most likely need a warrant to obtain more invasive details such as her personal messages and private data.

The prosecution would still have to authenticate the evidence under Fed. R. Evid. 901 which states that to satisfy the requirement of authenticating or identifying an item of evidence, the proponent must produce evidence sufficient to support a finding that the item is what the proponent claims it is.[32] While most of the data taken from cell phones are now more intangible, some tangible form of proof can always be presented in court to show that the data documentation (like GPS coordinates, stored information, messages, call logs) comes from the cell phone.

Mistakes leading to mistaken convictions occurring from misuse of expert testimony in digital data cases is an issue. In 2013, law enforcements in the U.S. made more than 1 million requests for American mobile phone data, a number that is growing.[33] In some of these cases digital data is misapplied.[34] The purpose of both sides, prosecution and defense being allowed to submit their

---

[31] *Id.*

[32] USCS Fed Rules Evid R 901. [Reproduced in the accompanying CD at Source 9]

[33] Ed Markey United States Senator for Massachusetts Report. For Second Year in a Row, Markey Investigation Reveals More Than One Million Requests By Law Enforcement for Americans Mobile Phone Data. December 9, 2013. Located at http://www.markey.senate.gov/news/press-releases/for-second-year-in-a-row-markey-investigation-reveals-more-than-one-million-requests-by-law-enforcement-for-americans-mobile-phone-data [Reproduced in the accompanying CD at Source 38]

own expert witnesses should allow both sides to address the misapplication of expert testimony.

B. Search warrants and restrictions of preliminary to admission of digital data as evidence in the UK and standard followed by EU countries.

The UK has fairly strict standards for data protection of individuals. UK's Data Protection Act,[35] passed in 1998 to address the explosion of personal data across a global Internet is still enforced. The Act states that everyone must follow a code of data protection principles, including the government, corporations, and organizations. The data should be:

- used fairly and lawfully
- used for limited, specifically stated purposes
- used in a way that is adequate, relevant and not excessive
- accurate
- kept for no longer than is absolutely necessary
- handled according to people's data protection rights
- kept safe and secure
- not transferred outside the UK without adequate protection

There is stronger legal protection for more sensitive information, such as:

- ethnic background

---

[34] Roberts v. Howton, 13 F. Supp. 3d 1077 (D. Or. 2014) [Reproduced in the accompanying CD at Source 18]

[35] https://www.gov.uk/data-protection/the-data-protection-act. [Reproduced in the accompanying CD at Source 30]

- political opinions
- religious beliefs
- health
- sexual health
- criminal records[36]

Evidence in the UK often needs to be relevant to the crime itself or a proper defense to the crime and, if necessary, show attribution. In the case In Clinton,[37] the defendant was accused of killing his wife. Here, evidence was properly attributed to the suspect, but was still not admitted. Here, the defendant, after using Facebook and pulling up his wife's Internet search history discovered she had been having affairs. After he confronted his wife, she callously told him to kill himself. He wanted to submit the Internet history documenting his wife's affairs and his own Internet history documenting his searches regarding suicide methods, to show that he had planned a murder suicide. He also wanted computer evidence submitted to show that his wife was having an affair. Although the magistrate ultimately did not allow the evidence because the evidence went to an improper defense: loss of self-control, the magistrate did not have an objection to the evidence from an authentication standpoint. [38]

In Suleiman, the prosecution had to attribute evidence of phone calls to the suspect[39]. Here,

---

[36] *Id.*

[37] 2012] 3 WLR 515, [2013] QB 1, [2012] EWCA Crim 2, [2012] Crim LR 539, [2012] 2 All ER 947, [2012] 1 Cr App R 26 (17 January 2012). *Located at* *http://www.bailii.org/ew/cases/EWCA/Crim/2012/2.html* [Reproduced in the accompanying CD at Source 34]

[38] *Id.*

[39] Suleman v. R[2012] EWCA Crim 1569. July 12, 2012. England and Wales Court of Appeal.

the defendant was suspected of placing hoax calls and starting fires at the same time. This case was especially difficult because the phone calls (hoax calls) needed to be linked to the fires (arson) as well. The suspect denied having the model of the phone used to make the call. His disclaimer was difficult to counter because he had an alibi for some of the fires and the case relied on both aspects of the evidence, hoax calls and arsons alibis, to be satisfied. When the police found the model of the phone in the suspect's home during a warrant search, the suspect claimed he did not own the phone and did not have any knowledge of its presence in his house.[40] Ultimately, the court allowed evidence of forensic experts who used voice recognition to link the suspects voice to the phone used to make the hoax calls that were placed at the time of the arson. In this case, the human attribution element (i.e the attribution of the phone calls to a specific person) was necessary for the prosecution to show to the magistrate because the defendant claimed he was not linked to the phone and in doing so, shifted the burden of proof to the prosecution with his disclaimer.

Overall, UK laws have similar barriers to searching personal cell phone and computer data compared to U.S. limitations. The current UK laws allow police officers to search personal data from phones only after an arrest. However, the UK allows more personal invasion restrictions for people crossing into or out of the UK. In this case, border patrol is authorized to take, hold, and examine cell phones, computers, and similar electronic devices under the UK terrorism Act of 2000.[41] This Act was created for the purpose of limiting terrorism and, while the UK may have a different definition of terrorism than the STL, the overall principle of the Act could be

---

(Criminal Division) Decisions. [Reproduced in the accompanying CD at Source 32]

[40] *Id.*

[41] Terrorism Act of 2000. Schedule 7. Located at http://www.legislation.gov.uk/ukpga/2000/11/contents [Reproduced in the accompanying CD at Source 33]

carried over to apply to the Office of the Prosecutor as well. The defendants on trial at the STL are all suspected of committing acts of terrorism.

UK courts allow courts to use cell phone data to corroborate evidence and attribute evidence to specific persons. In the UK, cell phone forensic analysis companies exists for sole purpose of gathering cell phone evidence and supplying expert witnesses to explain the data in court.[42] The forensic experts use systems that avoid corrupting already existing data, show how the data can be linked or not linked to a specific person and present their findings in court. The companies must still operate and attribute evidence to people within the confines of the law. The Association of Chief Police Officers created a guide for how to handle digital evidence, which has been adopted by most of the United Kingdom.[43] This guide lists specific principles of digital evidence in Section 2 such as:

- **Principle 1:** No action taken by law enforcement agencies, persons employed within those agencies or their agents should change data which may subsequently be relied upon in court.
- **Principle 2:** In circumstances where a person finds it necessary to access original data, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.
- **Principle 3:** An audit trail or other record of all processes applied to digital evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.
- **Principle 4:** The person in charge of the investigation has overall responsibility for ensuring that the law and these principles are adhered to.[44]

---

[42] Afentis Forensics. http://afentis.com/expert-witness/about/ [Reproduced in the accompanying CD at Source 35]

[43] ACPO Good Practice Guide for Digital Evidence. Association of Chief Police Officers. Adopted by Police Forces in England, Wales, and Northern Ireland. 2012. Located at http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=4&ved=0CDEQFjAD&url=http%3A%2F%2Fwww.digital-detective.net%2Fdigital-forensics-documents%2FACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf&ei=4PUrVfK3E4TfsASIp4HADg&usg=AFQjCNFC7xajX8s_4yk5Sif9MvalLf4hig&sig2=8HPhKoYW6W0mjVZj47DmTg&bvm=bv.90491159,d.cWc&cad=rja [Reproduced in the accompanying CD at Source 28]

[44] *Id.* at Section 2.

This guide also establishes that digital data is held to the same laws and rules that apply to documentary evidence.[45] Police have to use reasonable judgement after an arrest to take cell phones and use cell phone evidence factoring in issues like if the phone was found on the suspect (currently in use for the crime) or in a drawer.[46] The guidelines are thorough and explanatory and are updated regularly. The guide is seen as a benchmark for experts to ensure the evidence can be presented in court; UK forensic companies often guarantee that their experts follow these APCO guidelines.[47]

Digital data standards for forensic use vary within domestic courts.

Technical attribution is not that hard for most computers or phones. Most computers have an Internet signature specific to that device when online, the computer IP address. Network-level addresses also known as IP addresses are a useful starting point for attribution of evidence.[48] Cell phones with Internet connection are also traceable and have an online presence. Phone companies keep records of data and call use in storage, and, while this length of storage time varies by country, most large cell phone companies keep customer information. The

---

[45] ACPO Good Practice Guide for Digital Evidence. Association of Chief Police Officers. Explanation of the Principles. Section 2.2.1. Adopted by Police Forces in England, Wales, and Northern Ireland. 2012. Located at http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=4&ved=0CDEQFjAD&url=http%3A%2F%2Fwww.digital-detective.net%2Fdigital-forensics-documents%2FACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf&ei=4PUrVfK3E4TfsASIp4HADg&usg=AFQjCNFC7xajX8s_4yk5Sif9MvalLf4hig&sig2=8HPhKoYW6W0mjVZj47DmTg&bvm=bv.90491159,d.cWc&cad=rja [Reproduced in the accompanying CD at Source 28]

[46] *Id at* Section 4.3.

[47] Afentis Forensics. http://afentis.com/telephone-evidence/cell-site-analysis/. [Reproduced in the accompanying CD at Source 35]

[48] ESSAY: Untangling Attribution, 2 Harv. Nat'l Sec. J. 531, 532. [Reproduced in the accompanying CD at Source 42]

European Union, until recently, had a mandatory data retention policy. The 2006 Data Retention Act, which mandated that all telecommunications and ISP providers retain information on users for a minimum of six months, was overturned in 2014.[49] There are various ways to go online and use the Internet undetected such as Tor[50] or the deep web, but, because these online interactions are currently not traceable, they are not attributable to any technical device or person for the purposes of this paper.

Once the data has been tied to a device, the difficult part is tying that user to that particular device. For example, most cell phones have GPS capabilities that report information back to the service provider. GPS tracking is much more accurate than pinging location information from a cell tower, and is often time-stamped whereas the cell tower will give phones a recurring ping throughout the day. The cell phone geographic data can be corroborated with video or other documented footage from nearby areas. Phones that sync to a person's email or cloud storage devices are also a good indication of ownership. Even if defendants disclaim cell phones as their property, corroborating evidence can show phone recognition, as well as forensic syntax markers for messages and texting. While cell phone data and cell phone law has changed drastically since the 2005 terrorist bombings in Lebanon, it may behoove the STL to adopt the most recent standards for forensic analysis when creating a digital evidence policy. While not all the terrorists in 2005 used 2015 technology, the newer standards encompass older technology as well. The standards set out in the APCO guide need to be regularly updated, but that is to keep up with newer types of technology.[51] The APCO guidelines can still apply to older 2005 digital

[49] https://www.eff.org/node/81899. [Reproduced in the accompanying CD at Source 44]

[50] Tor Project. https://www.torproject.org/. [Reproduced in the accompanying CD at Source 43]

[51] ACPO Good Practice Guide for Digital Evidence. Association of Chief Police Officers. Explanation of the Principles. Section 2.2.1. Adopted by Police Forces in England, Wales, and Northern Ireland. 2012. Located at

data.[52]

IV. Conclusion

Evidence attribution varies among domestic states and is often tied to and restricted by warrant issues. Attribution evidence of digital data does not have a clear determination in domestic courts like the U.S. and the U.K; however, proper procedure is a common theme in both domestic courts. If the cell phone evidence was obtained without a warrant, the courts are much less likely to admit the evidence. In the U.S., digital data attribution is mostly a Fourth Amendment issue. U.S. courts almost always require a warrant and while the government can conduct searches without a warrant in certain cases like vehicular searches this privilege does not extend to government searches of data on private cell phones in vehicles. Additionally, in the U.S., search incidents to arrest no longer cover searches of cell phones. Sometimes, evidence relating to digital data can be admitted during expert testimony or data forensic analysis.

Attributing a certain technological device, like a cell phone or computer to a message or packet of information sent by phone or Internet is not that difficult on a forensic level, and a series of checkpoints for linking that device to the defendant with the data exists. Attributing that data on the device is much more problematic. Even if the device has been used by a suspect in the past or is registered to the suspect does not necessarily mean that the suspect is the owner of that device. If the court does not automatically attribute the device to the defendant, the defendant will most likely disclaim ownership of the device and the data sent from that device,

---

http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=4&ved=0CDEQFjAD&url=http%3A%2F%2Fwww.digital-detective.net%2Fdigital-forensics-documents%2FACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf&ei=4PUrVfK3E4TfsASIp4HADg&usg=AFQjCNFC7xajX8s_4yk5Sif9MvalLf4hig&sig2=8HPhKoYW6W0mjVZj47DmTg&bvm=bv.90491159,d.cWc&cad=rja [Reproduced in the accompanying CD at Source]

[52] *Id.*

and the burden of proof shits to the prosecution. The prosecution must show through some type of forensic analysis that show that human to data attribution. While there is no one good standard across domestic courts, the use of reasonable care in digital data attribution is a recurring issue. The Special Tribunal can ensure it follows in the spirit of what other domestic courts are trying to accomplish by looking ensuring it follows proper evidentiary procedure by: obtaining warrants, properly authenticating the digital data trail to specific persons, and following guidelines similar to those set out in the APCO Good Practice Guide for Digital Procedure.