

11-15-2020

Junk Evidence: A Call to Scrutinize Historical Cell Site Location Evidence

Victoria Saxe

Follow this and additional works at: https://scholars.unh.edu/unh_lr



Part of the [Evidence Commons](#)

Repository Citation

Victoria Saxe, *Junk Evidence: A Call to Scrutinize Historical Cell Site Location Evidence*, 19 U.N.H. L. Rev. 133 (2020).

This Notes is brought to you for free and open access by the University of New Hampshire – Franklin Pierce School of Law at University of New Hampshire Scholars' Repository. It has been accepted for inclusion in The University of New Hampshire Law Review by an authorized editor of University of New Hampshire Scholars' Repository. For more information, please contact sue.zago@law.unh.edu.



Victoria Saxe

Junk Evidence: A Call to Scrutinize Historical Cell Site Location Evidence

19 U.N.H. L. REV. 133 (2020)

ABSTRACT. Historical cell site location information (CSLI) has been offered as objective, scientific location evidence in criminal trials, but is far less precise than the claims it is used to support. Not only is there no way to pinpoint a cellphone’s precise geographic location from historical CSLI, but there are also no known validation or error rates for the methodologies used to collect and analyze this data. A 2019 telecommunications scandal in Denmark revealed gross inadequacies in the cellphone data and software used by law enforcement to analyze this type of evidence. The scandal sent shockwaves through the country’s legal community and led to a temporary moratorium on the use of cellphone location evidence, a comprehensive investigation into data collection and analysis practices, and the adoption of extensive reform and improvement measures. Perhaps even more importantly, the scandal undercut the trust and acceptance previously afforded to this type of evidence. Taking from the lessons learned in Denmark, this Note attempts to lay out what is known and unknown about historical CSLI and how the current state of this type of evidence comports with the Federal Rules of Evidence. In Part I, this Note first examines how and why historical CSLI is produced. Part II summarizes the current known issues with this type of cellphone location evidence. Finally, Part III sets forth the evidentiary shortcomings of historical CSLI that may be raised in criminal trials.

AUTHOR. University of New Hampshire School of Law, J.D. Candidate 2021. Sincerest thanks to Professor Buzz Scherr for his “annoying and supportive” guidance throughout the writing process and to *The University of New Hampshire Law Review* staff for their diligent review and helpful edits.

INTRODUCTION 135

I. UNDERSTANDING HISTORICAL CSLI & ITS LIMITATIONS..... 136

 A. *How Cellphones Operate in Cellular Networks* 138

 B. *How CSLI is Collected* 139

 C. *How CSLI is Analyzed* 142

II. PROBLEMS WITH HISTORICAL CSLI EVIDENCE 145

 A. *Unknown Accuracy of Underlying Data* 145

 B. *Cellphones Do Not Always Connect to the Closest Cell Tower*..... 149

 C. *Untested Methods of Analysis* 150

III. CHALLENGING THE ADMISSIBILITY OF HISTORICAL CSLI EVIDENCE 152

 A. *Federal Rules of Evidence Rule 702 – Testimony by Expert Witnesses* 153

 B. *Federal Rules of Evidence Rule 803(6) – Hearsay and the Exception for Business Records*..... 156

 C. *Federal Rules of Evidence Rule 901 – Requirement of Authentication* 158

 D. *Federal Rules of Evidence Rule 403 – Excluding Relevant Evidence for Prejudice or Confusion* 159

IV. CONCLUSION 160

INTRODUCTION

In June 2019, authorities in Denmark discovered errors in the way cellphone location data had been used in criminal trials in the country beginning in 2012.¹ Among the errors found, officials discovered that a flaw in the software used by police to analyze cellphone evidence omitted key location data collected by phone companies and linked phones to incorrect cellphone towers.² This meant that cellphones were sometimes linked to towers located hundreds of miles away from where the phone was at the time of the call.³ Denmark’s “telecommunications data scandal” shook the country’s trust in its legal system and led to the review of over 10,000 court verdicts, the release of 32 prisoners, and a two-month ban on the use of cellphone location data in criminal trials.⁴ When announcing this response to the discovered errors, Denmark’s Director of Public Prosecutions explained, “[w]e simply cannot live with the idea that information that isn’t accurate could send people to prison.”⁵

Denmark’s telecommunications scandal prompted an external investigation into its use of cellphone location data.⁶ This led the national police to adopt an entirely new infrastructure for handling cellphone data and implement routine independent quality control and data validation.⁷ It also prompted Norway to investigate its own use of cellphone location data.⁸

¹ IT-Pol, *Danish Data Retention: Back to Normal After Major Crisis*, EUROPEAN DIGITAL RIGHTS (Nov. 6, 2019), <https://edri.org/danish-data-retention-back-to-normal-after-major-crisis/> [<https://perma.cc/BD4Z-KNXT>].

² Louise Dalsgaard & Emma Toft, *Understand the Mistakes in the Telecommunications Scandal: Telephone Was in Copenhagen and Frederikshavn at the Same Time*, DANISH BROAD. CORP. (Aug. 31, 2019, 8:45 AM), <https://www.dr.dk/nyheder/indland/forstaa-fejlene-i-teleskandalen-telefon-var-i-koebenhavn-og-frederikshavn-paa-samme>, [<https://perma.cc/CR7H-5HJD>].

³ *Id.*

⁴ Jon Henley, *Denmark Frees 32 Inmates Over Flaws in Phone Geolocation Evidence*, GUARDIAN (Sep. 12, 2019 6:13 AM), <https://www.theguardian.com/world/2019/sep/12/denmark-frees-32-inmates-over-flawed-geolocation-revelations> [<https://perma.cc/TKP3-YRH9>]; Martin Selsoe Sorensen, *Flaws in Cellphone Evidence Prompt Evidence of 10,000 Verdicts in Denmark*, N.Y. TIMES (Aug. 20, 2019), <https://www.nytimes.com/2019/08/20/world/europe/denmark-cellphone-data-courts.html> [<https://perma.cc/AGE6-3Z2F>].

⁵ Henley, *supra* note 4.

⁶ IT-Pol, *supra* note 1.

⁷ *Id.*

⁸ ASSOCIATED PRESS, *Norway to Review Criminal Cases with Danish Telecom Data*, FED. NEWS NETWORK (Aug. 29, 2019, 5:37 AM) <https://federalnewsnetwork.com/world-news/2019/08/norway-to-probe-criminal-cases-with-danish-telecom-data/> [<https://perma.cc/T2SR-U2GA>].

The Denmark scandal underscores what critics have been saying about cellphone location evidence for years: using cellphone records to prove a criminal defendant's physical location is junk science.⁹ Yet, cellphone location evidence is used in tens of thousands of criminal cases in the United States each year.¹⁰ In Denmark, the country's mindset about cellphone data has changed.¹¹ This scandal – along with our understanding of the imprecision of cellphone location data, the unknown reliability of the methods used to collect and analyze this data, and the risk that juries will overvalue the accuracy of this evidence – should not be ignored. No country should be comfortable with the idea that inaccurate evidence could send people to prison.

I. UNDERSTANDING HISTORICAL CSLI & ITS LIMITATIONS

Nearly 96% of Americans owned a cellphone in 2019.¹² The vast majority of cellphone owners frequently carry their phones with them, and most never or rarely turn their phones off.¹³ Each day, the average cellphone user both makes and receives six phone calls and 32 text messages.¹⁴ Even the Supreme Court has had

⁹ See, e.g., Mark Hansen, *Prosecutors' use of mobile phone tracking is 'junk science,' critics say*, ABA J. (June 1, 2013, 8:50 AM), https://www.abajournal.com/magazine/article/prosecutors_use_of_mobile_phone_tracking_is_junk_science_critics_say [<https://perma.cc/RPY2-EVEY>]; Jeff Chinn, *Mobile Phone Tracking = Junk Science?* CALIFORNIA INNOCENCE PROJECT, Jun. 4, 2013, <https://californiainnocenceproject.org/2013/06/mobile-phone-tracking-junk-science/> [<https://perma.cc/TL96-P7TA>].

¹⁰ Albert Fox Cahn, *Phone Tracking Data is Notoriously Unreliable. So Why Are We Still Using it in Court?*, DAILY BEAST (Sep. 16, 2019 5:24 AM) <https://www.thedailybeast.com/denmarks-geolocation-data-crisis-could-prompt-a-reckoning-in-the-us-criminal-justice-system> [<https://perma.cc/3GS7-TURQ>].

¹¹ Henley, *supra* note 4 (quoting Karoline Normann, Head of the Danish Law Society's Criminal Law Committee) ("This situation has changed our mindset about cellphone data. We are probably going to question it as we normally question a witness or other types of evidence, where we consider who produced the evidence, and why and how.")

¹² Mobile Fact Sheet, PEW RES. CTR. (June 12, 2019), <https://www.pewresearch.org/internet/fact-sheet/mobile/> [<https://perma.cc/8T84-KQEX>].

¹³ Lee Rainie & Kathryn Zickuhr, *Chapter 1: Always on Connectivity, Americans' Views on Mobile Etiquette*, PEW RES. CTR. (Aug. 26, 2015), <https://www.pewresearch.org/internet/2015/08/26/chapter-1-always-on-connectivity/> [<https://perma.cc/A2JL-JRNA>].

¹⁴ *No Time to Talk: Americans Sending/Receiving Five Times as Many Texts Compared to Phone Calls Each Day, According to New Report*, PR NEWSWIRE (Mar. 25, 2015, 1:40 PM), <https://www.prnewswire.com/news-releases/no-time-to-talk-americans-sendingreceiving-five-times-as-many-texts-compared-to-phone-calls-each-day-according-to-new-report-300056023.html> [<https://perma.cc/LM9J-GS4Q>].

occasion to note that “modern cell phones . . . are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy.”¹⁵

The prevalence of cellphone use and advancements in phone technology have made cellphones a growing source of evidence in criminal cases.¹⁶ Evidence from cellphones can take many forms – including information like text messages, photos, and e-mail, as well as billing records of phone activity and use.¹⁷ Frequently, cellphones are used to provide crucial evidence in criminal cases to place a defendant at the time and place of a crime.¹⁸

The three most common ways cellphones are used to determine location are through Global Positioning System (GPS) technology; triangulation, a process used to estimate the location of a phone based on the cell tower locations of where its signal registers; and analyzing historical cell site location information or CSLI from a cellphone user’s call records.¹⁹ Though GPS and triangulation are considered quite accurate in determining a cellphone’s location, both methods typically require collecting information in real time.²⁰ Given the practical reality that most crimes are investigated after the fact, law enforcement frequently relies on historical CSLI, “the least accurate method of tracking a cell phone,” to hypothesize a defendant’s location when the alleged crime occurred.²¹ This Note considers CSLI – the use and analysis of cellphone call detail records and historical cell site location information – evidence which “is fraught with potential misunderstandings by courts and juries alike.”²²

¹⁵ *Riley v. California*, 573 U.S. 373, 385 (2014) (holding that a search warrant is required to search a cellphone even when phones are seized incident to arrest).

¹⁶ LARRY E. DANIEL & LARS E. DANIEL, *DIGITAL FORENSICS FOR LEGAL PROFESSIONALS: UNDERSTANDING DIGITAL EVIDENCE FROM THE WARRANT TO THE COURTROOM* 263 (Robert Maxwell & Sue Spielman eds., 2012).

¹⁷ *Id.* at 19.

¹⁸ John B. Minor, *Forensic Cell Site Analysis: A Validation & Error Mitigation Methodology*, 12 J. DIGIT. FORENSICS, SECURITY & L. 33, 34 (2017).

¹⁹ Thomas J. Kirkham, Comment, *Rejecting Historical Cell Site Location Information as Unreliable Under Daubert and Rule 702*, 50 U. TOL. L. REV. 361, 372 (2019); Rajiv Netra, *How GPS, Cell Tower and Wi-Fi Triangulation Help in Tracking Location?*, SAFETRAX (Sept. 5, 2017), <https://www.safetrax.in/2017/09/05/gps-cell-tower-triangulation-help-tracking-location/> [https://perma.cc/HUA8-WN7X].

²⁰ Kirkham, *supra* note 19, at 373. The privacy and Fourth Amendment implications of real-time GPS and triangulation tracking are not addressed in this Note.

²¹ *Id.* at 361–62.

²² Daniel & Daniel, *supra* note 16, at 225.

A. *How Cellphones Operate in Cellular Networks*

Cellphones work by sending and receiving radio signals between the phone's internal antennas and cell towers.²³ Cell towers are one part of the system of equipment and technology that facilitates cellular networks.²⁴ This system also includes transceiver stations, located at the base of every cell tower, which connect the radio signals from cellphones to radio network controllers, and mobile switching centers, which connect to all of the cell towers in a coverage area.²⁵ Every communication from a cellphone is routed through a mobile switching center and then onto the other phone with which it is communicating.²⁶

When a cellphone is first turned on, it attempts to "register" with a cellular network by sending a radio signal to the cell tower with the strongest signal.²⁷ There are hundreds of thousands of cell towers (also known as cell sites) in the United States – ranging from the tall, metal radio tower masts to antennas on raised structures like rooftops and billboards.²⁸ Given the large number of cell tower sites, a cellphone is usually no more than a few miles from a tower that it can connect to.²⁹ However, depending on the capabilities of the phone, internal cellphone antennas have the capacity to send radio signals to towers several miles away, potentially up to over 20 miles.³⁰

Cell towers typically provide coverage to circular areas with a few-miles' radius,

²³ *Id.* at 229–30.

²⁴ *Id.* at 226.

²⁵ *Id.* at 228.

²⁶ *Mobile Switching Center (MSC)*, TECHOPEDIA (Nov. 29, 2011), <https://www.techopedia.com/definition/8448/mobile-switching-center-msc> [<https://perma.cc/443V-UEZA>]; *Cellular Network*, TECHOPEDIA (Sept. 12, 2011), <https://www.techopedia.com/definition/24962/cellular-network> [<https://perma.cc/JZ35-9S8E>].

²⁷ Daniel & Daniel, *supra* note 16, at 229.

²⁸ Linda Hardesty, *China Tower Counts 1.95M Tower Sites, Dwarfing US Tower Sites*, FIERCE WIRELESS (Oct. 4, 2019 2:42 PM), <https://www.fiercewireless.com/wireless/china-tower-counts-1-95m-tower-sites-dwarfing-us-tower-sites> [<https://perma.cc/R7HY-8H32>]; *Cell Tower Industry Facts & Figures 2016*, VERTICAL CONSULTANTS, <https://www.celltowerleaseexperts.com/cell-tower-lease-news/cell-tower-industry-facts-figures-2016/> [<https://perma.cc/L4AG-M8SN>] (last visited Mar. 6, 2020).

²⁹ Bert Markgraf, *How Far Can a Cell Tower Be for a Cellphone to Pick Up the Signal?* CHRON.: SMALL BUS., <https://smallbusiness.chron.com/far-can-cell-tower-cellphone-pick-up-signal-32124.html> [<https://perma.cc/ZR8C-JQ7P>] (last visited Mar. 6, 2020).

³⁰ *Id.*

but the coverage area can vary in both distance and radius.³¹ For example, small towers in office buildings or airports may only have a coverage radius of 250 yards, while large cell tower structures can cover a range of ten miles or more in rural settings.³² And although some towers are designed to provide coverage to circular areas, others are designed to provide coverage in linear areas such as along a stretch of highway.³³ The breadth of coverage areas leads to overlapping zones, meaning in a given location, a cellphone is usually within the coverage reach of multiple cell towers.³⁴

It is a common misconception that a cellphone connects to the cell tower physically closest to it when registering to a cellular network.³⁵ On the contrary, the cellphone connects to the cell tower emitting the strongest signal.³⁶ Many factors affect the signal strength between a cellphone and the cell tower it connects to, including the number of available cell sites, which can be affected by repairs and maintenance; the technical characteristics of the tower, antenna, and phone; the weather, topography, and population density of the area; and whether the phone is being used indoors or outdoors.³⁷ This variability means it is possible for two cellphones – subscribed to the same cellular provider and in the exact same location – to place calls at the same time and connect to two different cell towers.³⁸

B. How CSLI is Collected

When a cellphone sends or receives radio signals from a cell tower, the

³¹ Daniel & Daniel, *supra* note 16, at 226, 233; Mark F. Rewers, *How to Find Your Nearest Cell Tower Locations*, UBER SIGNAL (Apr. 5, 2018), <https://www.ubersignal.com/blog/cell-tower-locations/> [https://perma.cc/HKZ4-4F6P].

³² Michael Harris, *How Cell Towers Work*, UNISON (2011), <http://www.unisonsite.com/pdf/resource-center/How%20Towers%20Work.pdf> [https://perma.cc/Q45C-EYZ4].

³³ Kirkham, *supra* note 19, at 369.

³⁴ *Id.*

³⁵ Douglas Starr, *What Your Cell Phone Can't Tell the Police*, NEW YORKER (June 26, 2014), <https://www.newyorker.com/news/news-desk/what-your-cell-phone-cant-tell-the-police> [https://perma.cc/UM9E-SA37].

³⁶ Daniel & Daniel, *supra* note 16, at 229–30.

³⁷ Aaron Blank, *The Limitations and Admissibility of Using Historical Cellular Site Data to Track the Location of a Cellular Phone*, 18 RICH. J.L. & TECH., Fall 2011, at 1, 7.

³⁸ Tom Jackman, *Experts Say Law Enforcement's Use of Cellphone Records Can be Inaccurate*, WASH. POST (June 27, 2014), https://www.washingtonpost.com/local/experts-say-law-enforcements-use-of-cellphone-records-can-be-inaccurate/2014/06/27/028be93c-faf3-11e3-932c-0a55b81f48ce_story.html [https://perma.cc/JB79-AA8M].

registration “ping” is processed through databases of account user information in mobile switching centers.³⁹ As a cellphone signal connects to a cell tower, the cellular network learns the tower location of the phone and then determines whether the phone has an active account that can receive and make calls.⁴⁰ While it is turned on, a cellphone will continue to periodically ping the tower with the strongest signal so that it remains registered to the system and can be located for incoming calls.⁴¹ This allows a cellphone to maintain registration to a network or connection for a call while a person is moving or driving, or while other factors affecting signal – like weather or cell traffic – fluctuate.⁴²

Cellular network equipment collects user and network information from these registration pings, including the account, date, time, and tower location receiving the signal.⁴³ However, because cellphone users are not billed for merely connecting to a network, cellphone carriers have no use to store the information from these registration pings beyond a few hours.⁴⁴ When a cellphone is used to place or receive a call or text message, cellular providers record the information collected by network equipment for customer billing and network monitoring purposes.⁴⁵ This “historical” metadata of cell activity, such as phone calls and text messages that pass through mobile switching centers, are retained by cellular companies for at least 18 months, as opposed to the mere hours the registration pings are stored.⁴⁶

When requested, cellular companies can generate billing records and CDRs with various data collected by the company.⁴⁷ The contents of CDRs can vary based on the carrier and the information requested, but typically show “details of the call such as the origination and destination addresses of the call, the time the call started and ended, the duration of the call ... [and] other billings associated with the call.”⁴⁸ CDRs also indicate the identification number of the cell tower that the phone

³⁹ Daniel & Daniel, *supra* note 16, at 230.

⁴⁰ *Id.*

⁴¹ *Id.*

⁴² *Id.*

⁴³ *Id.*

⁴⁴ *Id.*; Kirkham, *supra* note 19, at 372.

⁴⁵ Daniel & Daniel, *supra* note 16, at 225, 232.

⁴⁶ *Id.* at 163; *see also* 47 C.F.R. § 42.6 (2020).

⁴⁷ Daniel & Daniel, *supra* note 16, at 163–65, 232.

⁴⁸ Monique C.M. Leahy, *Telecommunications and Other Litigation: Call Detail Records and Fraud*, in 97 AM. JUR. TRIALS 1 § 1 (2020).

connected to during the registered activity.⁴⁹ The information about tower location contained in CDRs is generally referred to as cell site location information or CSLI.⁵⁰

CDRs are different from the actual billing statement that a carrier sends to its customers, which translates the metadata of codes and strings of numbers from CDRs into readable information about phone activity related to charges based on the customer's service plan.⁵¹ When a CDR is requested by an individual or agency⁵², cellular providers produce a record showing the requested data fields and information about how to decipher the included data.⁵³ To illustrate:

The following is a fictitious example of a call detail record:

```
E00QQ_5E|MTC1TST0000QQ5ESS000007200000084200000065200402292348347787
555891178755577180078759000000000000000634100000155IoN000000081700000000
000000000000000000000000000000000000000000000000000000000000000088400000868
```

This CDR indicates the date of the call (20040229), the time of the call (2348347, i.e., 11:48:34.7 pm), the calling number (7875558911), the called number (78755577180), the carrier identifier (0155), the billable time of the call (00000868, i.e., 868 tenths of seconds or one minute and 26.8 seconds), and other numbers including the switch name and trunk group.⁵⁴

Though the tower location recorded on the CDR merely indicates that the phone was somewhere within the signal coverage radius of the tower during the recorded activity, many claims are made as to what police and prosecutors can glean from the data embedded in CDRs.⁵⁵ Indeed, “[a]s early as 1999, cellular carriers began to produce Call Detail Records (CDR)/Cell Site Location Information (CSLI) evidence in response to subpoena, search warrants, and court orders.”⁵⁶ However, the claims made based on the information in CDRs are frequently “overstated”:

One of the most important things to remember is that a cell phone *cannot* be located from a historical call detail record. The best that can be done is that the phone can be placed in a general area corresponding to a cell tower that was connected to the phone

⁴⁹ Daniel & Daniel, *supra* note 16, at 232–33.

⁵⁰ Minor, *supra* note 18, at 33.

⁵¹ Daniel & Daniel, *supra* note 16, at 231; Leahy, *supra* note 48.

⁵² The Electronic Communications Privacy Act (ECPA) controls disclosure of call detail records and requires a court order, search warrant, or the subscriber's consent to release. 18 U.S.C. § 2703 (2019).

⁵³ Daniel & Daniel, *supra* note 16, at 164–64.

⁵⁴ Leahy, *supra* note 48.

⁵⁵ Daniel & Daniel, *supra* note 16, at 231–32.

⁵⁶ Minor, *supra* note 18, at 33.

at a particular time when a call was made or attempted.⁵⁷

Moreover, CDRs do not record the other cell towers that the phone was within range of or how far the cellphone was from the tower associated with the call to allow for a more precise triangulation of the phone's location.⁵⁸ And notably, CDRs cannot record who used the cellphone to make the registered activity.⁵⁹ Though this information would certainly be helpful evidence in criminal cases, CDRs are merely records used by cellphone companies "for the purpose of financial transactions such as generating bills to the subscriber and ... settling accounts with other carriers."⁶⁰ This is because "the cellular system was not designed to locate cellular phones beyond simply knowing if a cellphone can be reached to connect a call."⁶¹

Not only do CDRs contain limited information, but the accuracy of the information they contain is relatively unknown.⁶² Neither cellular carriers nor the Federal Communications Commission (FCC), which maintains cell site licensing filings, has documented error rates or validation methodologies for CDR or CSLI records.⁶³ Thus, it is generally unclear how accurate the actual location information in these records is before it is then subjected to external analysis.⁶⁴

C. How CSLI is Analyzed

Historical cell site analysis is the process of using cellular network information to analyze and interpret the recorded cell site location information in CDRs to approximate a cellphone user's past location.⁶⁵ Historical CSLI cannot be interpreted from CDRs alone.⁶⁶ The analysis involves interpreting the data from CDRs, like the identification numbers of the cell tower locations used by a phone number at specific times, against additional information from cellphone providers corresponding to the cell tower identification numbers, like coverage maps, configurations, and maintenance records for cell towers.⁶⁷

⁵⁷ Daniel & Daniel, *supra* note 16, at 231–32.

⁵⁸ Blank, *supra* note 37, at 13.

⁵⁹ *Id.* at 18.

⁶⁰ Daniel & Daniel, *supra* note 16, at 163.

⁶¹ *Id.* at 225.

⁶² Minor, *supra* note 18, at 35.

⁶³ *Id.*

⁶⁴ *Id.* at 34–35.

⁶⁵ Minor, *supra* note 18, at 33.

⁶⁶ Daniel & Daniel, *supra* note 16, at 163–64.

⁶⁷ *Id.*

1. CSLI Mapping and Software

The primary method of analyzing historical CSLI involves creating maps of cell site locations showing estimated cell site coverage areas where registered cellular activity could have occurred.⁶⁸ Essentially, analysts compare the times and cell tower locations recorded in CDRs with records from the cellphone company about cell tower locations, coverage, and maintenance history.⁶⁹ The analyst then maps out the coverage area of the identified cell towers and uses what she knows about the tower's configuration and signal to estimate where the registered cellphone activity could have occurred.⁷⁰ Given the amount of interpretation involved, mapping has “varying levels of accuracy” and “often provid[es] an unreliable interpretation of the actual evidence.”⁷¹

The easiest and most common way CSLI is analyzed is by inputting the data from CDRs and carrier records into mapping software that generate maps of cell tower locations and approximate where a cellphone could have connected to a cell tower during a given call.⁷² The availability of mapping software can expedite analysis of CDR and CSLI data.⁷³ Law enforcement, for example, often use commercial software to analyze historical CSLI.⁷⁴ One such software company advertises that it can map up to 4,000 calls in the time it would take to map one call by hand.⁷⁵ These programs are also used to generate visual aids and maps at trial.⁷⁶ But the ability to press an “easy button” and automatically map CSLI means that individuals conducting historical cell site analysis may only know how to use the software and may not know how to properly analyze CDRs, interpret carrier records, or understand the limitations of CSLI the way they would if conducting this

⁶⁸ Minor, *supra* note 18, at 33–34.

⁶⁹ Daniel & Daniel, *supra* note 16, at 164.

⁷⁰ *Id.*

⁷¹ Minor, *supra* note 18, at 33–34.

⁷² Larry Daniel, et al., *Are There Really Flaws in Cell Phone Location Evidence?*, ENVISTA FORENSICS (Oct. 7, 2019), <https://www.envistaforensics.com/blog/are-there-really-flaws-in-cell-phone-location-evidence/> [<https://perma.cc/Y476-6RD3>]. See generally *Basic Historical Cell Site Analysis Course Presented by FBI CAST, EVANSVILLE POLICE* (Nov. 2018), <http://evansvillepolice.com/sites/default/files/Basic%20Historical%20Cell%20Site%20Analysis%20Course.pdf> [<https://perma.cc/2VE5-4CJV>].

⁷³ *Id.*

⁷⁴ *Id.*

⁷⁵ *Benefits*, HAWK ANALYTICS, <http://www.hawkanalytics.com/benefits/> [<https://perma.cc/H9U2-5MUF>] (last visited Mar. 8, 2020).

⁷⁶ *Id.*

process manually.⁷⁷

2. Forensic Radio Surveys/Drive Tests

Another method used to analyze historical cell site information involves conducting a forensic radio survey or “drive test.”⁷⁸ Drive testing “is a method used by wireless telephone companies and radio frequency engineers to determine the coverage range of a cell tower for the purpose of determining the health of the telephone company’s wireless network.”⁷⁹ When employed by law enforcement, it can test whether “at the time of the drive test and in the location of the drive testing equipment, a phone can make an outgoing call and the phone can ‘hear’ a signal from a cell tower.”⁸⁰

The process begins by analyzing the data from CDRs and network information about the corresponding cell site locations to determine the general area where the recorded cellular activity could have occurred.⁸¹ Then, an analyst drives through the area while operating mobile receiver equipment to measure the signal strength of all towers in the area.⁸² The results from a drive test can be used to validate information from a CDR and areas of interest to show “that a cell phone could be at a particular place and would prefer the cell site and sector that was recorded in the historical call detail records.”⁸³ Alternatively, drive test results can be used to “create a map showing the limits of where a cell phone could be and connect to a cell tower or sector.”⁸⁴ However, given all the factors that affect signal strength and the unlikelihood that the weather and cellular network conditions during the test drive are identical to those when the cellular activity actually occurred, the reliability of this methodology is disputed.⁸⁵

⁷⁷ Daniel et al., *supra* note 72.

⁷⁸ *United States v. Morgan*, 292 F. Supp. 3d 475, 478–79 (D.D.C. 2018) (citing LARRY DANIEL, *CELL PHONE LOCATION EVIDENCE FOR LEGAL PROFESSIONALS: UNDERSTANDING CELL PHONE LOCATION EVIDENCE FROM THE WARRANT TO THE COURTROOM* (Academic Press 2017, 1st ed. 2017)).

⁷⁹ *Id.*

⁸⁰ *Id.*

⁸¹ *Id.*

⁸² *Id.*

⁸³ LARRY DANIEL, *CELL PHONE LOCATION EVIDENCE FOR LEGAL PROFESSIONALS: UNDERSTANDING CELL PHONE LOCATION EVIDENCE FROM THE WARRANT TO THE COURTROOM* 76 (Academic Press, 1st ed. 2017).

⁸⁴ *Id.*

⁸⁵ *Kirkham*, *supra* note 19, at 377; *Compare Phillips v. State*, 233 Md. App. 184, 189–90 (Md. Ct.

II. PROBLEMS WITH HISTORICAL CSLI EVIDENCE

Forensic cell site analysis is used regularly in criminal cases in the United States and is viewed as a “primary means of establishing [defendant location] evidence.”⁸⁶ Though it is often regarded as scientific and objective proof of such evidence, the accuracy of cell site analysis is highly variable and remarkably unvalidated.⁸⁷ The unreliability of this evidence, and consequently the risk of it being overly utilized in criminal investigations and trials, has caught the attention of courts,⁸⁸ legal scholars,⁸⁹ and media⁹⁰.

The criticism of historical cell site location analysis ranges from calls that it is “junk science” that should be excluded from any use in criminal trials,⁹¹ to calls for ensuring proper use that includes disclaimers of its limitations.⁹² The consensus among legal scholars seems to recognize the limitations of historical cellphone location evidence and to agree that such evidence cannot be used to pinpoint a phone’s precise location.⁹³ However, as long as this evidence is used in criminal trials, its limitations and admissibility must be better understood by attorneys, courts, and juries.

A. *Unknown Accuracy of Underlying Data*

1. Call Detail Records

First, historical cell site analysis depends on interpreting data collected by cellular companies in CDRs and in documentation of network infrastructure, maintenance, and system performance also produced by cellular companies.⁹⁴ As

Spec. App. 2017) (reviewing lower court’s conclusion that drive tests were not found to be generally accepted in the digital forensic science community or subject to peer-review), *with* United States v. Morgan, 292 F. Supp. 3d 475, 479 (D.D.C. 2018) (finding the methodology of drive testing to be generally reliable).

⁸⁶ Minor, *supra* note 18, at 34.

⁸⁷ *Id.*

⁸⁸ See, e.g., Hon. Paul W. Grimm, *Admissibility of Historical Cell Phone Location Evidence*, 44 No. 4 LITIG. 53 (Summer 2018).

⁸⁹ See, e.g., Kirkham, *supra* note 19; and Blank, *supra* note 37.

⁹⁰ See, e.g., Starr, *supra* note 35; GlobeNewswire, *Does Cell Phone Location Data Make for Bad Evidence?* YAHOO! FINANCE (Feb. 9, 2020), <https://finance.yahoo.com/news/does-cell-phone-location-data-013308219.html>, [<https://perma.cc/E3CD-FBP8>].

⁹¹ Hansen, *supra* note 9.

⁹² Daniel et al., *supra* note 72.

⁹³ See sources cited *supra* notes 86–87.

⁹⁴ Daniel & Daniel, *supra* note 16, at 163–64.

discussed above⁹⁵, these records are collected by cellular companies for billing, coverage, and analytics purposes, but are routinely used for much graver purposes against criminal defendants.⁹⁶ These are clearly incongruent interests in ensuring the accuracy of the location information collected. Additionally, cellular providers have never documented error rates or validation methodologies for the following records regularly used in historical cell site analysis:

1. Carrier cell site location database records.
2. CDR/CSLI records.
3. Documented network infrastructure and operational failures.⁹⁷

So, the first limitation in forensic cell site analysis is evident before the analysis even begins: the data that is being analyzed comes from unvalidated records of cellular network operations and unvalidated information about cell tower locations collected by phone companies for network billing purposes.⁹⁸ Practically speaking, it is uncertain how accurate the data in a CDR is – meaning we do not know whether cellular systems accurately record the identification number of the cell tower used to place a call 100% of the time or 99% of the time or less. Currently, law enforcement and courts rely on the underlying data contained in CDRs as if it is 100% accurate.⁹⁹ This ignores the possibility for errors in equipment glitches when recording cellular activity data and in the process of compiling usable data into CDRs.

The possible inaccuracy of CDR data was highlighted in the widely popular 2014 podcast “Serial,” which investigated the 1999 murder of Hae Min Lee in Baltimore, Maryland, and the ultimate conviction of Lee’s ex-boyfriend Adnan Syed.¹⁰⁰ At trial, cellphone records showing that Syed’s phone pinged a cell tower near the park where the victim’s body was found “played a significant role in the State’s case and the jury’s decision-making process.”¹⁰¹ However, in the wake of the podcast’s spotlight on the case, it was discovered that a fax cover sheet accompanying the

⁹⁵ See *infra* Part I, B.

⁹⁶ Minor, *supra* note 18, at 33.

⁹⁷ *Id.* at 35.

⁹⁸ See generally Minor, *supra* note 18.

⁹⁹ *Id.* at 35.

¹⁰⁰ Justin Fenton & Tim Prudente, *Adnan Syed Case: Maryland High Court Reinstates ‘Serial’ Subject’s Conviction*, BALT. SUN (Mar. 8, 2019, 6:15 PM), <https://www.baltimoresun.com/news/crime/bs-md-ci-syed-appeal-20190222-story.html> [<https://perma.cc/35NN-M9W2>].

¹⁰¹ Syed v. Maryland, Case No. 199103042-046, 1, 56 (Balt. Cir. Ct. 2016); Jon Swaine, *Serial’s Adnan Syed: Doubts Over Cellphone Evidence Central to Retrial*, GUARDIAN (Jul. 1, 2016, 12:38 EDT), <https://www.theguardian.com/tv-and-radio/2016/jul/01/serial-adnan-syed-new-trial-hae-min-lee-murder> [<https://perma.cc/G9SA-G8V6>].

“Subscriber Activity Report”¹⁰² used at Syed’s trial contained an explicit disclaimer about the reliability of its cell site location data.¹⁰³ The instructions stated: “Outgoing calls only are reliable for location status. Any incoming calls will NOT be reliable for location.”¹⁰⁴ Presumably, this meant that the carrier’s report generated cell tower information that did not necessarily correspond with incoming calls. The need for the disclaimer could have stemmed from unreliable cellular technology or known errors in the carrier’s system at the time the calls were made.¹⁰⁵ In either event, the disclaimer and the limitation of the location data from the records were not introduced by the state or challenged by Syed’s defense attorney.¹⁰⁶ Syed’s initial petition for postconviction relief was granted based on his trial attorney’s failure to cross-examine the state’s witness about the disclaimer and the reliability of the relied upon records.¹⁰⁷ This decision was ultimately reversed on procedural grounds.¹⁰⁸

2. Cellular Network Records

The second source of underlying data used in historical cell site analysis also comes from cellular network providers – “cell site location database records” and “[d]ocumented network infrastructure and operational failures.”¹⁰⁹ These records include the cellular company’s list of cell tower identification numbers and current locations, the coverage areas and configurations for each tower, and maintenance records for cell towers and other cellular equipment.¹¹⁰ This supplemental information is needed for analysts to interpret the calls and recorded cell tower

¹⁰² Though the state attempted to differentiate the term “Subscriber Activity Report” from “call detail records” to argue the disclaimer did not apply to the document relied on at trial, the cellphone carrier records at issue contained call activity and cell tower location information in the way of “call detail records” as discussed by this Note. *Syed v. Maryland*, Case No. 199103042-046 at 50–51.

¹⁰³ *Syed v. Maryland*, Case No. 199103042-046 at 40.

¹⁰⁴ *Id.*

¹⁰⁵ See Christina Everett, *5 Key Findings from ‘Undisclosed’ that ‘Serial’ Missed*, ENTERTAINMENT WEEKLY (Aug. 24, 2015, 12:00 PM), <https://ew.com/article/2015/08/24/5-key-finding-undisclosed-serial-adnan-syed/> [<https://perma.cc/64VJ-Q3DA>] (hypothesizing “[o]ne of the reasons for this disclaimer was due to a glitch with AT&T at the time, which had incoming calls ping the tower near the person making the call rather than the person on the receiving end.”).

¹⁰⁶ *Syed v. Maryland*, Case No. 199103042-046 at 40.

¹⁰⁷ *Id.* at 59.

¹⁰⁸ *State v. Syed*, 204 A.3d 139 (MD Ct. App. 2019).

¹⁰⁹ *Minor*, *supra* note 18, at 35.

¹¹⁰ *Daniel & Daniel*, *supra* note 16, at 163–64; *Minor*, *supra* note 18, at 37.

number listed in CDRs.¹¹¹ Again, cellular companies produce and retain this information for their own network monitoring and planning and have documented neither error rates nor validation methodologies for these records.¹¹²

One research project found that verifying the geographic cell site locations from the records produced by cellular carriers can “eliminate[] a substantial percentage of errors” in cell site analysis.¹¹³ In the study, “a cellular carrier produced records in response to a search warrant that erroneously identified more than 20 cell site locations within a radius of 2 miles.”¹¹⁴ Essentially, the cellular carrier provided incorrect information about the locations of its own cell sites due to documentation errors in its records of cite installation and equipment upgrades.¹¹⁵

The possibility of inaccurate cellular network records is not hypothetical: incorrect cell tower location data provided by cellular companies was one of the issues contributing to Denmark’s telecommunications data scandal.¹¹⁶ Denmark’s National Police explained the discovery that:

[T]he telecom providers’ mast¹¹⁷ lists have not been correct and continuously updated, and [] there have therefore been errors in the telecommunications providers’ historical lists of the telematers’ locations.

This could be, for example, because a telecommunications company has set up temporary masts due to repairs to existing masts, or because there is a festival in an area which therefore needs extra masts as there are more people gathered in one place.¹¹⁸

Inaccurate cellular network records compromise the reliability of historical cell site analysis because “[w]hen cell site locations are not validated[,] the preliminary analysis mapping risks introduction of false positive indications of the general location of the [phone].”¹¹⁹ In Denmark, the discovery of this problem led national police to establish a new collaboration with telecommunication companies to ensure accuracy in the records they provide police.¹²⁰ Until such action is taken in

¹¹¹ *Id.*

¹¹² Minor, *supra* note 18, at 35.

¹¹³ *Id.* at 37.

¹¹⁴ *Id.*

¹¹⁵ *Id.*

¹¹⁶ Dalsgaard & Togt, *supra* note 2.

¹¹⁷ The term “mast” refers to cellular network antenna equipment, which this Note refers to generally as “cell towers.” See Kirkham, *supra* note 19, at 370.

¹¹⁸ Dalsgaard & Togt, *supra* note 2.

¹¹⁹ Minor, *supra* note 18, at 37.

¹²⁰ Danish Minister of Justice, *Facts About Measures in the Telecom Data Case*, Press Release (Oct. 4,

the United States, attorneys should be prepared to challenge any cell site analysis conducted without this crucial validation step.¹²¹

B. Cellphones Do Not Always Connect to the Closest Cell Tower

Assuming cellular carrier equipment correctly records the data about a call and assuming this data is correctly transcribed in a CDR that is analyzed against accurate cellular network records, this only means that a cellphone was able to connect to a cellphone tower at a specific moment in time. Because cellphones do not always connect to the cell tower that is physically closest but to the one with the strongest signal, this may or may not be probative of the phone's location.¹²² The potential risks of overvaluing a cell tower's location relative to the phone's actual location can be illustrated by the dangerous problems resulting from the reliance on tower-location in developments to the United State's 911 routing system.¹²³

The 911 system relies on the location of the cell towers used to place emergency calls to route callers to nearby dispatch centers.¹²⁴ This is essentially the same principle behind historical CSLI mapping, which hypothesizes a cellphone's location based on the tower used to make or receive a call.¹²⁵ The goal of the 911 system's use of cell tower location is to route calls to the closest "public safety answering point (PSAP)" so that emergency services can be dispatched to the caller's location as quickly as possible.¹²⁶ However, because the "location of the cell tower that handles the call ... may be some distance (varying from a few hundred feet to several miles) from the caller's location," a high volume of emergency calls are routed to the wrong dispatch center (dispatch centers that are closer to the cell tower than the caller's actual location).¹²⁷ For example, after sustaining a head injury, a pregnant woman called 911 from a playground in Burlington County, New Jersey, but the cell tower she connected to routed her to a dispatch center in

2019), <https://www.justitsministeriet.dk/nyt-og-presse/pressemeddelelser/2019/fakta-om-tiltag-i-teledatasagen> [<https://perma.cc/J362-WR44>]; "Lesson 7" in https://www.justitsministeriet.dk/sites/default/files/media/Pressemeddelelser/pdf/2019/faktaark_-_tiltag.pdf (last visited Sept. 8, 2020) [<https://perma.cc/C234-NW8V>] (*translated in Danish*).

¹²¹ See Minor, *supra* note 18, at 37.

¹²² Kirkham, *supra* note 19, at 368.

¹²³ *Id.* at 379.

¹²⁴ *Location-Based Routing for Wireless 911 Calls*, 33 FCC Rcd. 3238, 1 (Mar. 23, 2018).

¹²⁵ Kirkham, *supra* note 19, at 379.

¹²⁶ *Location-Based Routing for Wireless 911 Calls*, *supra* note 124.

¹²⁷ *Id.*

Philadelphia.¹²⁸ Emergency calls like this are not technically “misrouted,” because they are correctly routed to PSAPs closest to the tower location that facilitated the call; rather, the errors occur because the system relies on the fallacy that cellphones always connect to the nearest cell tower.¹²⁹

Tower-based routing results in delays in the delivery of emergency response services, leading to greater injuries and sometimes death.¹³⁰ The FCC has responded to the problem by enacting “Enhanced 911 rules” and new requirements for wireless carriers.¹³¹ It is believed that the FCC’s transition from “tower-based routing to location-based routing” could improve the reliability of 911 dispatch routing and save over 10,000 lives per year.¹³² Critics of the use of historical CSLI against criminal defendants have pointed to the 911 system as an example of the unreliability of cell towers to determine location.¹³³ The FCC’s recognition of the inadequacy of relying on cell towers in determining caller location has given further weight to the argument that “[a] methodology that has been determined by independent government agencies not to be able to stake a caller’s life on should not now be accepted as reliable enough to risk a defendant’s liberty.”¹³⁴

C. *Untested Methods of Analysis*

In addition to not knowing the reliability of the underlying data in CDRs, the methodologies used to analyze historical CSLI have only been tested by law enforcement.¹³⁵ This means that there are no known error rates to support the accuracy of CSLI mapping, software used to analyze historical CSLI, or drive tests. These methods of interpreting historical CSLI have only been implemented by law enforcement, the same party who is usually offering the evidence against a criminal defendant.¹³⁶ And just as CSLI and CDR data have been “acknowledged as accurate

¹²⁸ Kirkham, *supra* note 19, at 381.

¹²⁹ *Id.*

¹³⁰ *Id.*

¹³¹ *Enhanced 911 – Wireless Services*, FEDERAL COMMUNICATIONS COMMISSION, <https://www.fcc.gov/general/enhanced-9-1-1-wireless-services> (last visited Sept. 18, 2020) [<https://perma.cc/GFA3-8U3T>].

¹³² Kirkham, *supra* note 19, at 382.

¹³³ *Id.*

¹³⁴ *Id.* (citing Michael Cherry, et al., *Cell Tower Junk Science*, 95 JUDICATURE 151, 152 (2012)).

¹³⁵ Kirkham, *supra* note 19, at 377.

¹³⁶ *Id.* (“No one outside of law enforcement is testing these methods because no one outside of law enforcement uses these methods to track a phone.”).

by [] courts without any validation or error mitigation,”¹³⁷ courts have generally accepted the methods used to analyze this data merely because they are widely used by law enforcement.¹³⁸

A recent study in the U.S. exploring ways to improve accuracy in forensic cell site analysis recommended both validating the underlying CSLI and CDR data and set forth a multi-step methodology for analyzing this data.¹³⁹ The methodology combines many of the processes that are often independently relied on by law enforcement, and it also advises taking additional steps to promote accuracy and mitigate the errors that can result from inaccurate cellular network records and the impact of external factors that affect cell signal.¹⁴⁰ The proposed methodology recommends conducting drive tests, performing a topographic analysis, researching aggravating events that contribute to cell signal traffic, analyzing network infrastructure and traffic, researching historical weather conditions, analyzing network operations and maintenance records, analyzing cell carrier performance metrics, and researching cellular operating standards.¹⁴¹ The study found that these steps “resulted in a modified final mapping analysis in approximately 40% of the cases,” and even more significantly, that it “resulted in a modified final mapping analysis that impacted the outcome of the case in terms of the verdict of guilt or innocence in criminal cases or damages award in civil litigation” in 6% of cases.¹⁴²

The study also noted that “[a]lthough several specialty software tools purport to produce accurate analysis results, including mapping generated from CDR/CSLI evidence, none of the software tools currently perform the discovered evidence validation and analysis error mitigation methodology.”¹⁴³ With no other studies confirming the reliability of traditional CSLI analysis, this study suggests that as many as 40% of mapping analyses conducted by law enforcement using available commercial software could have underlying errors. It also suggests that inaccurate cell site analysis could be contributing to wrongful convictions in many of the tens

¹³⁷ Minor, *supra* note 18, at 35.

¹³⁸ Kirkham, *supra* note 19, at 376; see also Alexander Ransom, *FBI Historical Cell Site Analysis*, LAW OFFICE OF ALEXANDER RANSOM, PLLC, (Sept. 8, 2018), <http://ransom-lawfirm.com/fbi-historical-cell-site-analysis/> [<https://perma.cc/CTG4-P82H>] (discussing *State v. Ramirez*, 425 P.3d 534 (Wash. Ct. App. 2018) *cert denied*, 435 P.3d 266 (Wash. 2019)).

¹³⁹ Minor, *supra* note 18, at 35–36.

¹⁴⁰ *Id.*

¹⁴¹ *Id.* at 35.

¹⁴² *Id.* at 45–46.

¹⁴³ *Id.* at 47.

of thousands of criminal cases where historical CSLI evidence is used each year.

Denmark's telecommunications scandal again serves as a cautionary tale of using unvalidated methodologies to produce forensic evidence. It was, in fact, the discovery of "multiple glitches" in the software police had used to analyze CSLI data that prompted the country's moratorium on cellphone location evidence, the review of thousands of cases, and the discovery of even further flaws in the data and methodologies police were using.¹⁴⁴ One source of errors occurred where the "conversion algorithm" that was utilized to sync the geographical coordinates of cell sites cellular providers used with the ones police used, "was applied twice to some mobile tower data, which moved the geolocation positions by a couple of hundred meters."¹⁴⁵ The scandal also revealed that:

The IT system used for converting telecommunications data was developed internally by the police and maintained by a single employee. Before December 2018, there were no administrative practices for quality control of the data conversion system, not even simple checks to ensure the entire data received from mobile service providers had been properly converted.¹⁴⁶

Cellphone forensic experts have said that such errors "are actually quite common when automated software is used to analyze cellular call detail records without being verified or validated."¹⁴⁷ Nevertheless, challenges to unvalidated mapping software have been rejected by courts.¹⁴⁸

III. CHALLENGING THE ADMISSIBILITY OF HISTORICAL CSLI EVIDENCE

The limitations of correlating cellphone location with cell-tower location, the unknown accuracy of CSLI and CDR data, and the lack of validated and reliable methodologies to interpret historical CSLI create a dangerous predicament: untested and unvalidated evidence disguised as scientific and reliable evidence can make its way to juries in criminal trials. Until the United States is forced to overhaul the way this data is collected and analyzed as prompted by the Danish telecommunications scandal, the safeguards against unreliable evidence in the Federal Rules of Evidence can provide some bases for exclusion or heightened scrutiny. The following evidentiary issues should be considered when historical CSLI evidence is introduced against a criminal defendant.

¹⁴⁴ Henley, *supra* note 4.

¹⁴⁵ IT-Pol, *supra* note 1.

¹⁴⁶ *Id.*

¹⁴⁷ Daniel et al., *supra* note 72.

¹⁴⁸ See e.g., Ransom, *supra* note 138.

A. Federal Rules of Evidence Rule 702 – Testimony by Expert Witnesses

Testimony that is based on “scientific, technical, or other specialized knowledge” falls within the scope of expert testimony under Rule 702 of the Federal Rules of Evidence.¹⁴⁹ Courts are divided as to whether evidence about how cellphones connect to towers and how historical CSLI is analyzed requires expert testimony.¹⁵⁰ This means that in some courts, custodians of records for cellular companies and law enforcement officers – without training in cellular technology or the validity and reliability of CSLI and CDR data and analysis – can provide lay testimony about how historical CSLI places a defendant in proximity to a crime scene.¹⁵¹ This can result in misleading information and the introduction of apparently objective, technical information that has not been subject to the evidentiary standards typically required for expert testimony. Arguably, the line between what is permissible as lay testimony and what requires expert testimony should be drawn at “testimony that goes beyond the simple descriptions of cell phone basics, specifically testimony that purports to pinpoint the general area in which the cell phone user was located based on historical cellular data, requires scientific, technical, or other specialized knowledge.”¹⁵²

Rule 702 sets forth the requirements for testimony by expert witnesses.¹⁵³ The subparts of the rule and federal caselaw interpreting these requirements provide guiding factors for courts to use in assessing the reliability and admissibility of expert testimony.¹⁵⁴ Analyzed against these criteria, historical CSLI evidence may fail to meet the requirements of Rule 702.¹⁵⁵

Rule 702(a) specifies that a witness who is qualified by “knowledge, skill, experience, training, or education” may testify if this expertise “will help the trier of fact to understand the evidence or to determine a fact in issue.”¹⁵⁶ Individuals who introduce historical CSLI evidence must be able to explain how cellular systems

¹⁴⁹ FED. R. EVID. 702(a); see Kirkham, *supra* note 19, at 375.

¹⁵⁰ Grimm, *supra* note 88, at 54 (comparing e.g., United States v. Graham, 796 F.3d 332, 364-65 (4th Cir. 2015), with United States v. Natal, 849 F.3d 530, 533 (2d Cir. 2017)).

¹⁵¹ See e.g., State v. DePaula, 166 A.3d 1085, 1098, (N.H. 2017) (citation omitted) (holding that “custodians could testify as lay witnesses because they possessed sufficient personal knowledge to discuss generally the means by which cell phones connect to the closest tower and the general ranges of cell towers”).

¹⁵² Collins v. State, 172 So.3d 724, 743 (Miss. 2015); see also, Grimm, *supra* note 88, at 54–55.

¹⁵³ FED. R. EVID. 702.

¹⁵⁴ *Id.*

¹⁵⁵ See Kirkham, *supra* note 19, at 375–79.

¹⁵⁶ FED. R. EVID. 702(a).

operate, how cellphones connect to cell towers, the reliability of the data collected, and how the CSLI and CDR data was reliably analyzed. Though cellphones are ubiquitous and the average layperson may understand the basic way cell towers work, there are many aspects of historical CSLI evidence that are beyond the average cellphone user's experience, such as the variability of cell signal, the cellular network equipment and technology used to generate CDRs, and the methodology employed in analyzing CSLI and CDR data. Experts who are qualified to testify about the relationship between historical CSLI and a cellphone's approximate location may include electrical engineers¹⁵⁷ and law enforcement agents with "specialized training" and experience in conducting historical cell site analysis.¹⁵⁸ Attorneys should be prepared to challenge the qualifications of witnesses introducing cellphone location evidence, or to call their own experts to accurately explain the highly technical and variable aspects of CSLI data and analysis.

Rule 702(b) further requires that an expert's testimony be "based on sufficient facts or data."¹⁵⁹ This suggests that, as a prerequisite to providing testimony, the underlying data supporting an expert's opinion must be reliable. As discussed above, there are no known error rates for the CSLI data contained in CDRs or cellular network records used in CSLI analysis.¹⁶⁰ Denmark's telecommunications scandal and the Adnan Syed case suggest that incorrect data may form the basis of historical CSLI analysis in some instances. Unless the data contained in a CDR and its accompanying cellular network records have been externally validated, any subsequent analysis and testimony is arguably not based on "sufficient" data.¹⁶¹

Rule 702(c) next requires that the testimony be "the product of reliable principles and methods."¹⁶² In *Daubert v. Merrell Dow Pharmaceuticals, Inc.*, the Supreme Court set forth factors for determining "whether the reasoning or methodology underlying the testimony is scientifically valid and [] whether that

¹⁵⁷ *United States v. Banks*, 93 F. Supp. 3d 1237, 1251 (D. Kan. 2015) (finding "radio frequency engineer[s]" who worked for cellular company were qualified to provide expert testimony about defendant's approximate location based on cell site location data).

¹⁵⁸ *United States v. Jones*, 918 F. Supp. 2d 1, 4 (D.D.C. 2013) (noting federal agent's extensive and specialized training qualified him to provide expert testimony).

¹⁵⁹ FED. R. EVID. 702(b).

¹⁶⁰ *See infra* Part II, A.

¹⁶¹ *See* FED. R. EVID. 702(b); *see generally* *Stonefire Grill, Inc., v. FGF Brands, Inc.*, 987 F. Supp. 2d 1023, 1039 (C.D. Cal. 2013).

¹⁶² FED. R. EVID. 702(c).

reasoning or methodology properly can be applied to the facts in issue.”¹⁶³ These factors include (1) whether the methodology “can be (and has been) tested”; (2) whether it “has been subjected to peer review and publication”; (3) what the “known or potential rate of error” is; and (4) its “general acceptance” within relevant scientific communities.¹⁶⁴

As discussed above¹⁶⁵, the principles and methods used to analyze historical CSLI have not been tested or validated outside the law enforcement community, and there is no known error rate for the underlying data or methodologies used. At least one study¹⁶⁶ and the implications of the Danish telecommunications scandal suggest that unreliable methodologies for data collection and analysis exist. Currently, historical CSLI analysis is not used or accepted outside the law enforcement community, but using tower-location to determine physical location has been acknowledged as problematic by the FCC in its administration of the 911 system.¹⁶⁷ The “widespread acceptance” of historical CSLI by the law enforcement community – the very community offering this evidence – should not be mistaken for the reliability associated with acceptance by a “relevant scientific community.”¹⁶⁸ Although no factor identified in *Daubert* is dispositive¹⁶⁹, the current state of historical CSLI and analysis falls short in each category.¹⁷⁰ Until experts test these methodologies, subject them to further peer review and “the scrutiny of the scientific community,” and determine the potential error rates of data collection and analysis¹⁷¹, testimony based on CSLI mapping techniques and software is arguably not the product of “reliable” methods.

Finally, Rule 702(d) requires that the expert “has reliably applied the principles and methods to the facts of the case.”¹⁷² Assuming a properly qualified expert under 702(a) has externally validated the data in a CDR report to meet the requirements of 702(b), and then employed a reliable methodology to analyze the CSLI data to meet the requirements of 702(c), an issue under 702(d) may potentially

¹⁶³ *Daubert v. Merrell Dow Pharm., Inc.*, 509 U.S. 579, 592–93 (1993).

¹⁶⁴ *Id.* at 593–94.

¹⁶⁵ See *infra* Part II, A and C.

¹⁶⁶ See *Minor*, *supra* note 18.

¹⁶⁷ *Location-Based Routing for Wireless 911 Calls*, *supra* note 124.

¹⁶⁸ *Daubert*, 509 U.S. at 594 (citation omitted).

¹⁶⁹ See *id.* at 593, 594.

¹⁷⁰ See *Kirkham*, *supra* note 19, at 375–79.

¹⁷¹ *Daubert*, 509 U.S. at 593.

¹⁷² FED. R. EVID. 702(d).

still arise. However, given the current problems with unvalidated CSLI data and methodologies, proposed cellphone location evidence may not survive challenges under 702(a)-(c) to warrant further scrutiny under 702(d).

B. Federal Rules of Evidence Rule 803(6) – Hearsay and the Exception for Business Records

Out of court statements, including printed statements and records, are generally inadmissible under the Federal Rules of Evidence as “hearsay.”¹⁷³ However, CDRs offered as business records are frequently admitted by courts as an exception to the prohibition against hearsay under Rule 803(6) when “the underlying data is kept and maintained by a reliable computer program in the regular course of business.”¹⁷⁴ CDRs are essentially computer records¹⁷⁵ produced by cellphone companies for tracking “customer billing, carrier rates, for network monitoring, and for facility capacity planning.”¹⁷⁶ To qualify as a business record under 803(6), the following conditions must be met:

- (a) the record was made at or near the time by - or from information transmitted by - someone with knowledge;
- (b) the record was kept in the course of a regularly conducted activity of a business, organization, occupation, or calling, whether or not for profit;
- (c) making the record was a regular practice of that activity;
- (d) all these conditions are shown by the testimony of the custodian or another qualified witness, or by a certification that complies with Rule 902(11) or (12) or with a statute permitting certification; and
- (e) the opponent does not show that the source of information or the method or circumstances of preparation indicate a lack of trustworthiness.¹⁷⁷

¹⁷³ FED. R. EVID. 802.

¹⁷⁴ *People v. Zavala*, 156 Cal. Rptr. 3d 841, 843 (Cal. Ct. App. 2013).

¹⁷⁵ That CDRs are automatically generated by cellular network system computers does not affect their admissibility under the business records exception. *See* 1 JACK B. WEINSTEIN & MARGARET A. BERGER, WEINSTEIN’S EVIDENCE MANUAL § 16.07[2][g] (2020) (citing *United States v. Salgado*, 250 F.3d 438, 451-453 (6th Cir. 2001) (“trial court did not err in finding computer printout trustworthy when employee of company testified it represented type of record his company regularly generated and maintained in its files, and that his company relied on similar reports for billing purposes; fact that many entries were made by computer, rather than by human being, and witness’s lack of knowledge of error rate did not disqualify record for admission as business record.”)).

¹⁷⁶ Leahy, *supra* note 48, § 1.

¹⁷⁷ FED. R. EVID. 803(6).

The rationale for the business records exception is based on “reliability and need.”¹⁷⁸ Because records produced by businesses are regularly checked, consistently produced, relied upon by businesses, and compiled by employees whose employment incentivizes their attention to accuracy, these records are viewed as sufficiently trustworthy to overcome the rule against hearsay.¹⁷⁹

Defendants have tried (unsuccessfully) to challenge the admissibility of CDRs under the business records exception from several angles: objecting to the use of reports that are not generated during the course of business but in response to a request from law enforcement¹⁸⁰; objecting to a lack of foundation showing how the records were produced, identified, and stored¹⁸¹; and challenging the reliability or trustworthiness of the record.¹⁸² Although there is no known error rate or validation methodology for CSLI data collected by cellular companies or produced in CDRs, courts have generally treated these records as sufficiently trustworthy.¹⁸³ However, what is reliable for the business purposes of cellular carriers is not necessarily reliable for the purpose of proving a defendant’s location in criminal proceedings.

The fact that CDRs do not constitute hearsay under the business records exception does *not* address their admissibility under Rule 702 and *Daubert*.¹⁸⁴ “The former question goes to reliability of the statements contained therein; the latter question goes to the scientific reliability of the methodology that forms that basis of the statements.”¹⁸⁵ When offered as evidence for the limited purpose of a cellphone user’s calls or cellular activity, CDRs may be sufficiently reliable to be admissible

¹⁷⁸ 1 WEINSTEIN, *supra* note 175, at § 16.07[2][b].

¹⁷⁹ *Id.*

¹⁸⁰ See, e.g., *People v. Zavala*, 156 Cal. Rptr. 3d 841, 844–45 (Cal. Ct. App. 2003) (“[A Sprint records custodian] also described how he obtains those records in response to legal demands . . . Courts in other jurisdictions have considered this issue, and the majority of them conclude a printed compilation of data produced by human query for use at trial falls under the business records exception provided the underlying data is kept by a reliable computer software program in the regular course of business.”).

¹⁸¹ See, e.g., *People v. Bahena*, No. 213118, 2020 WL 133378, at *4 (Ca. Ct. App. 6th Dist. 2020) (citation omitted).

¹⁸² *State v. Wright*, No. 08-1737, 2010 WL 200052, at *8 (Iowa Ct. App. 2010).

¹⁸³ *Id.* at *8 (“Several courts have approved the use of cell phone and cell tower usage records in criminal cases as circumstantial evidence of the defendant’s approximate location . . . [o]ur view is no different.”) (internal citations omitted); *Minor*, *supra* note 18, at 35.

¹⁸⁴ See *State v. Kirsch*, 820 A.2d 236, 245 (Conn. 2003).

¹⁸⁵ *Id.*

under the business records exception.¹⁸⁶ But when offered as evidence of a defendant's location, CDRs are arguably still not admissible for the reasons discussed above.

Whenever the business records exception is cited for historical CSLI evidence, attorneys should be prepared to challenge the scientific reliability under Rule 702 and *Daubert*, as well as the adequacy of the foundation and authentication of the evidence. If admitted under the business records exception, attorneys should consider requesting a limited jury instruction that explains that the data is admissible only for the limited purpose of suggesting that a phone connected to a cell tower at a specific time.¹⁸⁷ This may then protect against jurors considering what is only sufficiently reliable to meet the business records exception as scientifically reliable evidence of a defendant's physical location.

C. Federal Rules of Evidence Rule 901 – Requirement of Authentication

The introduction of historical CSLI evidence also poses an issue for the evidentiary requirement of authentication.¹⁸⁸ Federal Rules of Evidence Rule 901(b) requires the proponent of evidence to “produce evidence sufficient to support a finding that the item is what the proponent claims it is.”¹⁸⁹ The rule goes on to list examples of evidence satisfying the requirement, which includes in subsection (9) “[e]vidence describing a process or system and showing that it produces an accurate result.”¹⁹⁰ The Advisory Committee Notes to this rule state that “Example (9) is designed for situations in which the accuracy of a result is dependent upon a process or system which produces it.”¹⁹¹ The accuracy of CDRs and historical CSLI evidence clearly depends on the method of analysis used to produce them. Thus, attorneys should be prepared to raise authentication challenges to CDRs that are not supported by evidence showing the carrier's system produced accurate historical CSLI data and (unlike the Syed case) that the information in the CDR “is what the proponent claims it is.”¹⁹²

¹⁸⁶ See Blank, *supra* note 37, at 51–54.

¹⁸⁷ See Kirkham, *supra* note 19 at 390.

¹⁸⁸ See Blank, *supra* note 37, at 53–54.

¹⁸⁹ FED. R. EVID. 901(a).

¹⁹⁰ FED. R. EVID. 901(b)(9).

¹⁹¹ FED. R. EVID. 901(b)(9) advisory committee's note to 1972 proposed rule.

¹⁹² FED. R. EVID. 901(a).

D. Federal Rules of Evidence Rule 403 – Excluding Relevant Evidence for Prejudice or Confusion

Since the early 2000s, the “CSI effect” has been described as a phenomenon influencing jury deliberations in criminal cases.¹⁹³ In response to the popularity of true crime and forensic television shows, the CSI effect is believed to “lead[] jurors to have unrealistic expectations of forensic tests and possibly cause them to incorrectly weigh the importance of either the absence or presence of forensic evidence.”¹⁹⁴ Though the effect is often cited by prosecutors who believe it creates a higher standard for the evidence they must demonstrate to yield a conviction, it is also believed to cause juries to be “more likely to convict based on a misinterpretation of forensic evidence.”¹⁹⁵

Authorities in Denmark cited the potential for jurors to overvalue forensic cellphone evidence when discovering the data and software flaws undermining the accuracy of cellphone location evidence.¹⁹⁶ Prior to the telecommunications scandal, cellphone location evidence was widely viewed as “highly accurate” and given “high significance and value in courtrooms because [it was] considered almost objective.”¹⁹⁷ The likely prejudice and confusion that unvalidated cellphone location evidence could create caused the country to take significant steps to control the use of this evidence.¹⁹⁸ There is also a risk that American juries may overly weigh cellphone location evidence as objective and highly accurate forensic evidence in criminal cases, despite the true accuracy of historical CSLI evidence being unknown and often overstated,¹⁹⁹ and this “objective” evidence being “in fact produced by the prosecution”²⁰⁰ offering it.

Rule 403 of the Federal Rules of Evidence is designed to serve as a gatekeeper to otherwise relevant evidence “if its probative value is substantially outweighed by a danger of one or more of the following: unfair prejudice, confusing the issues, [or]

¹⁹³ John Alldredge, *The “CSI Effect” and Its Potential Impact on Juror Decisions*, 3 THEMIS: RES. J. OF JUST. STUD. & FORENSIC SCI. 114, 115 (2015).

¹⁹⁴ *Id.*

¹⁹⁵ *Id.*

¹⁹⁶ Henley, *supra* note 4.

¹⁹⁷ *Id.*

¹⁹⁸ *Id.*

¹⁹⁹ Daniel & Daniel, *supra* note 16, at 231.

²⁰⁰ Mark A. Godsey & Marie Alou, *She Blinded Me with Science: Wrongful Convictions and the “Reverse CSI-Effect”*, 17 TEX. WESLEYAN L. REV. 481, 483 (2011).

misleading the jury... ”²⁰¹ The accuracy of cellphone location evidence is confusing and not fully understood, and the precision of tower-location data is misleading.²⁰² Despite this, juries who are presented with “forensic” cellphone evidence by “experts” are likely to view this evidence as highly accurate and objective.²⁰³ Thus, attorneys should be prepared to challenge the admissibility of cellphone location evidence under 403. Defendants who challenge the admissibility of cellphone location evidence under 403 should cite to the phenomenon of jurors overvaluing forensic evidence when arguing that any probative value in determining a defendant’s general location from historical CSLI is outweighed by the prejudice that would result from jurors failing to appreciate the lack of validation and unknown reliability of this evidence, as well as the confusing misconception that cellphone signals connect to the closest cell tower.²⁰⁴ A defendant’s 403 argument should also cite the risks inherent to expert testimony which “can be powerful, misleading, and difficult to evaluate” and thus deserves greater weight when assessing potential prejudice under 403.²⁰⁵ At the very least, attorneys confronting cellphone location evidence should proceed with caution as criminal attorneys in Denmark have been forced to do: “We are probably going to question it as we normally question a witness or other types of evidence, where we consider circumstances like who produced the evidence, and why and how.”²⁰⁶

IV. CONCLUSION

Cellphone location evidence has been offered as accurate by law enforcement and accepted as accurate by courts without any validation or proven reliability. There are several misconceptions about how cellphone technology works and how much information can truly be gleaned from historical CSLI data. The limited review of the methodologies used to collect and analyze cellphone location data and the 2019 telecommunications scandal in Denmark suggest that the ways law enforcement and prosecutors use CSLI data does not always produce accurate evidence of a defendant’s location. And still, cellphone location evidence is used in

²⁰¹ FED. R. EVID. 403.

²⁰² See *infra* Part II.

²⁰³ See Henley, *supra* note 4.

²⁰⁴ *But see* United States v. Morgan, 292 F. Supp. 3d 475, 485, 486 (D.D.C. 2018) (rejecting 403 challenge where defendant argued that the imprecision of cellphone location evidence and likely misconception that phones connect with the closest tower were misleading when testimony could be limited to a possible location within a general coverage area).

²⁰⁵ *Daubert*, 509 U.S. at 595 (citation omitted).

²⁰⁶ Henley, *supra* note 4.

tens of thousands of criminal trials each year.²⁰⁷

Although this evidence is widely permitted in criminal trials, the gaping holes in the sufficiency of the underlying data and reliability of the methodologies used to analyze historical CSLI create opportunities for evidentiary challenges to the admissibility of cellphone location evidence. Until the United States is forced to reckon with the limitations and risks of this data as prompted by the Danish scandal, challenges under Federal Rules of Evidence Rules 702, 901, and 403 should be raised to keep what is possibly junk science, and more likely junk evidence, from being introduced against defendants in criminal trials.

²⁰⁷ Cahn, *supra* note 10.