The Legal Impacts and Opportunities of NG911 Architecture: Transparency, Privacy, and Evidentiary Considerations

Authored by[*]*:*

Connor Boe, Jordan Demo & Alex Bibisi

[*] This paper was created as a research project with the University of Colorado Law School Samuleson-Glushko Technology Law and Policy Clinic. This work was developed in conjunction with advisors from the National Highway Transportation Safety Administration's National 911 Coordination Program, and consultants from Mission Critical Partners. A special thank you to our partners and advisors: Laurie Flaherty, National 911 Coordination Program; John Chiaramonte, Mission Critical Partners; Nancy Pollock, Mission Critical Partners; Colby Rachfal, Mission Critical Partners; Blake Reid, Samuelson-Glushko Technology Law and Policy Clinic.

Executive Summary

Data collection, analysis, and storage is cheaper and more reliable than ever before.[1] This advancement has substantially impacted 911 systems, which are dedicated to emergency response. With the advent of Next Generation 911 (NG911), the proliferation of data when responding to emergencies will inevitably increase in size and scope. Though the receipt, processing, analysis, and storage of more data in emergency responses will be beneficial for public safety, it may also create complexities for existing statutory and regulatory obligations. Specifically, these systems have the potential to complicate state open records law compliance, privacy and data protection obligations, and chain-of-custody rules of evidence. Policy makers, emergency services, and vendors of these services need to consider the legal implications before deploying NG911 systems and not after the fact. This piece attempts to discuss how the architecture of NG911 systems will impact how they interact with these existing legal obligations.

[1] *See* William D. Nordhaus, *The Progress of Computing*, SSRN (Sep. 27, 2001), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=285168 (Computing power from 1940 to 2001 grew on average by 55% per year); *see also* Nick Routley, *How the computing power in a smart phone compares to super computers in the past and present*, BUSINESS INSIDER (Nov. 6, 2017), http://www.businessinsider.com/infographic-how-computing-power-has-changed-over-time-2017-11 (There has been a 1-trillion-fold increase in computing performance over the last 60 years).

Table of Contents

Discussion

I. Introduction

The collection, storage, and computation of data has become cheaper and more reliable than ever before.[2] This increase in technological capability is having a significant impact on public safety in a number of ways. From the establishment of the First Responder Network Authority (FirstNet) to the use of Internet of Things (IOT) devices in emergency response, data is becoming an integral part of our national framework for emergency response and management.[3]

One technology that is being changed by the proliferation of data is the 911 emergency calling system. Legacy 911 systems only allow PSAPs to collect information based on voice communication with a caller at the scene of the emergency. This system is limited in terms of the amount of information a PSAP can discern about an emergency since the 911 telecommunicator must rely solely on the information conveyed in a voice call.

However, emerging technologies are enabling callers and PSAPs to exchange new types of information, including multimedia data and text communications. The advent of IOT devices (like medical devices, sensor devices attached to first responders, and automatic crash notification available on newer vehicles) allow for the passive collection of large quantities of data communicated via IP communication platforms.[4] Industry groups and public safety advocates have begun the process of envisioning, developing, and deploying systems for integrating this information as part of the emergency response purposes, known as Next Generation 911 (NG911).

NG911 is an Internet Protocol (IP)-based system that allows Public Safety Answering Points (PSAPs) to receive aggregate, analyze, and store diverse sets of critical information about an emergency incident. With this data, PSAPs can better prepare first responders in the field with a detailed picture of the emergency, thereby increasing efficiency of the response and improving outcomes.

There are slight differences in operational practices of NG911 systems and legacy 911 systems. In the legacy system 911 response, the only information about the crash that a PSAP can collect is the verbal information provided by callers on the scene and passersby. The information collected from these calls may be conflicting and contradictory, and it is difficult for a PSAP to gain a full picture of the scene of the accident. The PSAP communicates relevant information collected from

---

[2] *See id.*

[3] *See generally* Lili Yang, *How Internet of Things Technology Enhances Emergency Response Operations*, RESEARCHGATE (Nov. 2013), https://www.researchgate.net/publication/271880691_How_the_internet_of_things_technology_enhances_emergency_response_operations_Technological_Forecasting_and_Social_Change_809_1854-1867.

[4] Cecilia Murtagh & Gladys Klemic, *Internet of Things Networks for First Responders Report*, DEP'T. OF HOMELAND SEC. (Dec. 2015), https://www.dhs.gov/sites/default/files/publications/NUSTL%20OpEx%20Experimentation%20Report%202015%20Internet%20of%20Things%20Networks%20for%20First%20Responders.pdf.
(continued…)

callers to the first responders arriving on scene and the responders are left to sort out the details of the incident based on their real-time situational awareness. By way of example, a common use case for a NG911 system envisions a multicar pile-up on an interstate highway.[5]

In a NG911 world, the receiving PSAP equipped with a NG911 system could:

- Collect multimedia data from citizens at the scene;
- Collect video streaming from an unmanned aerial vehicle (UAV);
- Access traffic camera video and still images available at the incident site;
- Collect collision information from automatic crash notification systems in vehicles;
- Collect medical information of individuals involved including information from personal wearables
- Cross reference personal data from the individuals involved with an incident with medical records from the state wide medical record sharing systems;
- Access critical infrastructure information about the roads, utilities, and weather conditions; and
- Collect information about potential hazardous materials that may be involved in the accident.[6]

The receiving PSAP, with the assistance of machine learning or an individual in a dedicated position, could analyze this mass amount of data and communicate more reliable and pertinent information to the first responders arriving on scene. Rather than relying on the often conflicting information from callers and their own situational awareness, the real-time data analytics PSAP and first responders could use more reliable information from multiple sources to make determinations on an appropriate response. As a result, NG911 systems have the potential to make emergency response efforts faster, more efficient, and more effective.

While NG911 could have tremendous benefits for emergency response efforts, there may be e unanticipated consequences for state and local governments. The 911 community has already begun to acknowledge that the significant increase in data collection will likely create conflicts within government transparency, public safety concerns, and individual privacy.[7]

More specifically, NG911 technology and the magnitude of data that will be available on the incident is expanding the role of the PSAP in the first response framework by increasing the PSAPs need to aggregate multiple and diverse data sets and serve as an information filter between callers, first responders, and data collection technology that is available for emergency response. For the purpose of this analysis, it is helpful to think of legacy systems in a limited way where the legacy system is only able to collect certain discrete pieces information. This analysis assumes that current legacy systems and the PSAPs that operate them can only collect voice calls, and smaller pieces of

---

[5] *Broadband Implications for the PSAP: Analyzing The Future of Emergency Communications* 7-8, APCO INTERNATIONAL (2017), https://www.apcointl.org/ext/pages/p43/p43book.html#p=1) [hereinafter *APCO Report*].

[6] *Id.*

[7] *APCO Report, supra* note 5, at 50-55.

data like CAD reports and database queries. The reality is that these systems are designed differently and have different capabilities which would further complicate this analysis. In NG911 there are two variations of how NG911 systems can be architected.

The first version of the architecture contemplates a deployment of a massive system that collects all of the information discussed in the example above in a very centralized way. The PSAP would serve as a real-time public safety data analytics center where all of the information concerning an emergency will be aggregated, analyzed, and stored by a single vendor or agency. This means that the NG911 system is taking on additional obligations of not only collecting and storing voice calls and smaller discrete pieces of data but aggregating and analyzing this information. Furthermore, we can imagine that everything collected by a PSAP might be a part of a single data file, combining all of the aggregated data in a way that is not easily segregable.

The second deployment scenario would be less centralized in its implementation than the first. This system might be constructed in a way where all of the data that is collected is stored separately—perhaps by different entities, such as a PSAP and various first responders—or even if aggregated could be easily segregated into its constituent parts—e.g., audio recordings, telemetry data, health information, etc. In other words, the system could be architected in such a way that the data could be queried at a granular level.

These two architectures are not mutually exclusive but operate on a spectrum; there are a wide variety of ways a NG911 system could be configured. However, these two hypothetical architectures help frame the two extremes of how a system could be designed and how relevant legal considerations might apply.

There are considerations to both of these architectures that local governments and policy makers should be aware of. The more centralized version creates administrative synergies, and makes document retention and storage easier. Furthermore, it makes compliance easier as it relates to chain of custody obligations and data breach protections. With these benefits, there are also potential downsides, including the difficulty of complying with open records and protecting private information of individuals involved in 911 responses. The more decentralized version is beneficial because it makes ORL compliance and protecting private information easier.

This piece examines how NG911 systems might impact three areas of law relevant to emergency response framework:

- First, it discusses how NG911 architecture will impact State ORLs if deployed. Specifically, we discuss how the architecture of the system will change how we define what a "record" is, and how to apply statutory exemptions to these laws.
- Second, it discusses how NG911 architecture will impact privacy concerns of citizens including patient health information, state wiretap recording laws, and data breach obligations.
- Finally, it discusses how NG911 architecture and the proliferation of digital evidence can create interesting dynamics and complexities regarding authentication and chain-of-custody obligations for pending actions. Specifically, how information is stored, who stores it, and how digital evidence is tracked in this system can create complexities for authenticating evidence that is collected by these systems.

II. Open Records Laws (ORL)

Potential conflicts between government transparency, public safety, and personal privacy will become apparent with the implementation of NG911 in state ORLs. State ORLs require that state and local agencies allow "records" kept by agencies in the course of conducting government business to be inspected by the public.[8] All 50 states have some sort of ORL and many of these state ORL statues are modeled after the federal Freedom of Information Act, though go by different names depending on the state—e.g., Sunshine Laws, Freedom of Information Acts (FOIA), Right-To-Know Laws, etc.[9]

Open records laws embody governmental commitment to transparency, but that commitment is tempered by competing public interests of personal privacy, public safety, and national security.[10] As NG911 systems will be collecting information that concerns public safety and personally identifiable information (PII), it will become increasingly important for agencies involved in the administration of 911 systems to understand how to balance sensitive and private information with the public's right to know how their government operates.

Almost all states ORL administration operates the same way.[11] They function with a two-part inquiry is required to determine if a record is disclosable to, or protected from, disclosure to the public. First, a requester must identify what a "record" is according to the state statue, and if what is being requested meets the state's definition. If what the requester is asking for is in fact a "record" as defined by the state statute, the second part of the inquiry requires that the custodian or holder of the record determine if the record is exempted from disclosure based on the state statute and common law. Furthermore, if the record/records contain both exempted and disclosable information, then the state must determine if the record can reasonably be redacted to protect exempted information, or if the presence of exempted information makes the record wholly exempted.

The NG911system's architecture will influence how to determine what the relevant "record" is, and how to apply the various state exemptions to the record. How data is collected, stored, and retrieved may vary significantly across different implementations of NG911 systems, raising questions about the scope of the relevant "record" or "records."

The two aforementioned visions of NG911 data records architecture will have different consequences as they apply to ORL compliance from state to state. This section considers ORL compliance in the face of these two different forms of NG911 systems. First, we discuss how these two visions of NG911 technology associated with the data records architecture could operate in conjunction with "record" inquiry of ORLs. Depending on the architecture of the system, NG911

---

[8] *See Open Government Guide*, REPORTERS COMMITTEE FOR FREEDOM OF THE PRESS (2011), https://www.rcfp.org/open-government-guide [hereinafter *RCFP Open Government Guide*].

[9] 5 U.S.C. §552 (2012); *see also* Martin Halstuk & Bill Chamberlin, *The Freedom of Information Act 1966-2006: A Retrospective on the Rise of Privacy Protection Over the Public Interest in Knowing What the Government Is Up To*, 11 Comm. L. & Pol'y 511, 520 (2006).

[10] Memorandum from John Ashcroft, Attorney Gen., on the Freedom of Information Act to Heads of all Fed. Dep't and Agencies (Oct. 12, 2001), https://www.justice.gov/archive/oip/011012.htm.

[11] *See* Halstuk at 533.

related data systems could raise complicated questions about the scope of "records" covered under ORLs. Second, we discuss how record exemptions in ORLs that apply 911 calls may change in the NG911 data world based on how we define the "record" and what information is contained within the "record." Finally, NG911 data records policy may raise complex questions about the remedies plaintiffs may levy against PSAPs—both for failing to adhere to ORLs and for inadvertently disclosing protected information.

A. NG911 and the Scope of "Records"

Currently, almost all states recognize legacy recorded 911 voice calls as "records" that are disclosable to the public under ORLs.[12] One example statutory definition of a record comes from the Colorado Open Records Act (CORA), enacted in 1969 and patterned after the Federal Open Information Act.[13] Under CORA, a "public record" means "all writings made, maintained, or kept by the state . . . for use in the exercise of functions authorized by law."[14] CORA's definition of a "writing" is quite broad and includes "tapes, recordings, and other documentary materials, regardless of physical form."[15] Recorded 911 voice call records are disclosable under CORA unless the voice call contains information that is otherwise exempted from disclosure.[16]

Most legacy 911 systems only have the capability of collecting certain data from a caller, as most systems only allow a caller to contact a PSAP by voice call. However, in some areas, citizens can also contact a PSAP via text.[17]

Using the multicar pile-up scenario, a legacy 911 systems can only collect information given to the PSAP via voice or text communication with the individual who initiates a call. Under CORA (and many ORLs), the 911 voice recording is a "record" that might be disclosable to the public upon request.

However, the concept of a "record" becomes more complicated with regards to data in NG911 due to the potential of vast amount of data collected during NG911 communications. The collection and aggregation of more voluminous and diverse sets of data raises difficult questions about the scope of the relevant "record" or "records" under an ORL request.

First, the NG911 framework involves collecting a great deal of additional information beyond voice calls. For instance, the PSAP can collect information on an ongoing basis, even after the initial contact is concluded, through automated systems (e.g., city CCTV, onboard vehicle systems, state record automated queries, and UAV video). If all this additional data is stored as one data set, does that constitute one "record" or "multiple records" that would be subjected to ORLs? There is no

---

[12] *See generally RCFP Open Government Guide*, *supra* note 8 (approximately 41/50 states hold that 911 voice calls are subject to disclosure).

[13] Denver Post Corp. v. University of Colorado, 739 P.2d 874, 882 (Colo. App. 1987).

[14] Colo. Rev. Stat. § 24-72-202(6)(a)(I).

[15] Colo. Rev. Stat. § 24-72-202(7).

[16] Freedom of Colorado Information, Inc. v. El Paso County Sherriff's Dept., 196 P.3d 892, 898 (Colo. 2008).

[17] *Text 911 Master PSAP Registry*, FCC, www.fcc.gov/files/text-911-master-psap-registryxlsx (last visited Dec. 20, 2017).

doubt that all of the data collected during an incident response will be "a public record" subject to ORLs but, how the information is collected, stored, and retrieved will impact if the information is one "record" or multiple "records" This distinction matters for two reasons.

First, the administrability of storing and retrieving records on a relevant incident might become more complex. If all of the data is stored in one file or location containing everything collected during a NG911 call at one location, it will be easy to request the record. Having one place where this information is stored can decrease administration costs. Fewer resources will be needed to maintain the records and ORL requesters will only need to file one request for the relevant record. If, however, the data collected for a given response is stored in a granular way where different agencies are responsible for certain pieces of information and that information is stored in a highly segregable way, it could increase administration costs of compliance. For example, agencies will have to direct requesters to different locations for different piece of information and additional staff will be required to maintain the records. In addition, requesters may need to go to multiple agencies, file numerouse requests and track down many records for a single emergency response. This will make it much harder to determine where, how, and who a requester must ask for information on emergency responses.

Second, the distinction raises questions about how and when to apply statutory exemptions in a given state's ORL. The scope of an individual "record" will determine if an exemption applies to the record in question, if the government has the obligation to redact the record and disclose it, or if it is wholly exempted. Any information that is part of a "record" might be disclosable or might be exempted depending on the relevant state's law and how the record is interpreted.[18]

B. NG911 Data and ORL Exemptions

Though governments should be committed to transparency, there are circumstances in which transparency can harm the pursuits of public safety, protecting private information, and the disclosure of information that could jeopardize public service. These issues in disclosure are often protected by ORL exemptions.

Each state has its own regulationsfor exempting sensitive information from disclosure. Recorded 911 phone calls are treated very differently from state to state.[19] If someone requests the audio recording, the metadata of the phone call, or the text chain of an "emergency call", those are typically disclosable under ORLs in some form, but may be subject to certain constraints (transcript versus audio recording).[20] Some states expressly exempt 911 calls from disclosure, while other states subject 911 calls to disclosure but require redaction of certain information to protect the parties

---

[18] *See RCFP Open Government Guide* (discussing different statutory exemptions in each state and how to deal with so called "comingled" documents that contain both exempted and disclosable information).

[19] *911 Recordings & Transcripts-State Statutes*, NEWSEUM INSTITUTE (July 18, 2012), http://www.newseuminstitute.org/2012/07/18/911-recordings-transcripts-state-statutes (a more detailed list of the state exemptions for 911 calls.)

[20] *Id.*

(continued…)

involved or where a call includes otherwise non-disclosable information investigatory records, or content that would otherwise harm or embarrass the parties involved in the incident.[21]

One common exemption for 911 records applies to voice calls subject to an ongoing investigation that could jeopardize the integrity of that investigation, the investigatory procedures of the police department, or private information protected by other legal administrations.[22] Requests for legacy 911 calls often are subject to this exemption and withheld based on pending criminal or administrative action.[23] If the voice call contains information about a suspect, or evidence that will be used in a future trial against a criminal defendant, the call might be withheld from disclosure until the pending criminal or administrative investigation is concluded.

Colorado, for example, has a unique framework for determining whether records must be disclosed, including a complex "public interest" exception. While 911 calls meet the definition of a public "record" and are not expressly exempted from disclosure under a CORA request, CORA allows the custodian of "public records to deny the right of inspection if the disclosure would be contrary to the public interest."[24]

One specific area of disclosure that can be withheld from disclosure as contrary to the public interest includes:

> "Any records of investigations conducted by any sheriff, prosecuting attorney, or police department, any records of the intelligence information or security procedures of any sheriff, prosecuting attorney, or police department, or any investigatory files compiled for any other law enforcement purpose".[25]

This delineation between the "voice call" record and the "investigation" record(s) is much clearer in the legacy framework. The voice recording between the PSAP and the caller is a disclosable record, and its easier to determine if this voice recording contains information that is critical to an ongoing investigation due to the size and scope of the record. As a result, legacy 911 systems that only collect voice or text data have small records that take relatively limited resources to analyze and determine if the "investigatory" exemption would apply to the call.

---

[21] *Compare* Ala. Code § 11-98-12 (Supp. 2010) (expressly exempts 911 voice calls from disclosure), Cal. Gov't Code §6254(f)(1) (requires disclosure unless subject to an ongoing criminal investigation, *and* Ky. Rev. Stat. §61.878(1)(a) (requires the state to disclose 911 voice call unless the any exempted information is contained therein, specifically personally identifiable information); *see also, Bowling v. Brandenburg*, 37 S.W. 3d 785 (Ky. App. 2000) (finding that a 911 call containing personally identifiable information is not subject to the state ORL unless compromising information is redacted).

[22] *Id. E.g.*, Colo. Rev. Stat § 24-72-304(1); Ala. Code § 12-21-3(b); D.C. Code § 2-534(a)(3).

[23] *See generally* Jamison S. Prime, *A Double Barreled-Assault: How Technology and Judicial Interpretations Threaten Public Access to Law Enforcement Records*, 48 Fed. Comm. L.J. 341, 345 (1996).

[24] Colo. Rev. Stat. §§ 24-72-204(2)(I), 301(2); In re People v. Thompson, 181 P.3d 1143, 1143-44 (Colo. 2008) (clarifying that 911 calls are "public records" subject to CORA).

[25] *Id.*

(continued…)

Some other commonly exempted information under ORLs include private or confidential information, criminal records, personally identifiable information (PII), individual health information, financial information, or any information that can be seen as "against the public interest" if disclosed.[26] These "records" or pieces of information are exempted either by statue, common law, or municipal code and vary amongst the states. If this information is present within a record, the custodian or keeper of the record has to determine how to navigate their state ORL without compromising government transparency.[27]

These exemptions raise complex questions about how to deal with NG911 data and records that comingle disclosable information and exempted information in a common record. CORA and many other state ORLs require that when information that is exempted by state statue is comingled with information that is disclosable, the custodian of the record must take "reasonable efforts" to redact or segregate the information such that the record might still be disclosable.[28] NG911 systems contemplate aggregating much more information about an event at the PSAP including information that concerns public safety, personal privacy, and information subject to the public interest than legacy 911 voice calls.[29] The increase in the size and scope of information collected in NG911 makes the analysis more difficult and dependent on the architecture of the system.

C. Architecture Considerations

The centralized NG911 is more complicated because the data collected by the PSAP for an incident could be considered one "record." In this instance, it is easy to imagine that diverse set of information would be contained within the single "record"—i.e., the file containing all the data transferred to the PSAP.

For example, using the multi-car pile-up scenario, all of the information relayed to the PSAP would be stored together including multimedia data, health information, automatic crash notification information, city utilities information, and critical HAZMAT information. Some of this information would likely be considered exempt—e.g., health and investigation information—and other information would be disclosable—e.g., the audio recordings of callers.[30] The difficulty lies in whether the state requires an agency or holder of the record to redact or segregate disclosable information from exempted information.

---

[26] *E.g.,* CA, CO, PA, FL, CT, MI, TN, TX.

[27] *See, e.g.,* Globe Newspaper Co. v. Chief Med. Examiner, 404 Mass. 132, 134 (Mass. 1989) (if the disclosure of requested documents would "indirectly identify" affected parties, or the segregation of non-exempted portions would be too burdensome, the custodian of the record may withhold the records with a bona fide showing of potential harms).

[28] *Compare* Sargent School Dist. No. RE-33J v. Western Services Inc., 751 P.2d 56, 61 (Colo. 1988), Fla. Stat. § 119.07(1)(d) (to the extent a valid exemption has been asserted and applies to part of a public record, Chapter 119 allows that portion of the record to be redacted.), *and* Cal. Gov't Code § 6253(a)(California); *see also* 2 AAC 96.325(a)(1), .210(d), .330 (2006); Town of Trumbull v. FOIC, 5 Conn. L. Trib. No. 34, 38 (Conn. Super. Ct. 1979).

[29] *APCO Report, supra* note 5, at 52-55.

[30] *See id.* at 7-8.

(continued…)

This centralized NG911 data system may have the consequence of making even more 911 calls exempted based on investigatory exemptions and other common exemptions, as more information is aggregated about specific incident responses.[31] Information that was traditionally investigatory in nature, such as crime scene photos, officer body camera footage, telemetry data, etc., will be combined with the voice call, metadata, and other inherently disclosable information. As a result, the PSAP or designated custodian will have to go through the massive amounts of data and determine if the information can be reasonably redacted or segregated. If the information cannot be "reasonably" segregated or redacted, there is a possibility that all the information collected would be withheld based on the exemptions. This will undoubtedly create confusion of when the record is disclosable, and when the protected information contained the file is so prominent, that the entire file is not disclosable. [32]

Ssystems that aggregate data in a way that makes it difficult to segregate pieces of information could be a very burdensome, incident specific, and costly endeavor for many small PSAPs. These systems could lead to a decrease in transparency in emergency responses if the holders of the record (i.e. any agency who is tasked with storing and maintaining the digital records) systematically deny ORL requests on the premise that the data is comingled and it would be unreasonable to redact of segregate the information.

In the more decentralized version, where information collected during a NG911 call is stored in a way where the information is easily segregable into discrete pieces of data, the question of the "record" might change. In fact, each segregable piece of data might be treated as a separate "record" making it easier for the PSAP to withhold exempted information, and disclose information subject to the state ORL.

In this case, compliance with ORLs would be much easier on the PSAP. This architecture would ensure that discrete pieces of information can be retrieved, limiting the amount of work that a PSAP would need to conduct in redacting exempted information. However, this could create issues for data management in administering the records. If each of these granular pieces of information are stored separately at different agencies or with separate vendors, it might be harder to gain access to all information collected on a single incident. Compartmentalization could possibly create higher compliance costs with the need for more staff and resources to deal with ORL requests.

As the multi-car pileup scenario illustrates, there will be a great deal of information that flows over the network to the PSAP that was not available in legacy systems. [33] Though this aggregation of data may be tremendous benefit for public safety purposes during a response, it can create problems for ORLs if the architecture of the system is ignored before the deployment of a system. We refrain

---

[31] *Compare* Mo. Rev. Stat. § 610.100.2, Evening News Ass'n v. City of Troy, 417 Mich. 481, 497 (1983) (For a govt. entity to show investigatory report is exempted from disclosure, it must provide more than conclusory statements of conflict. The entity must show specifically how disclosure of certain documents would compromise and ongoing investigation), *and* O.C.G.A § 50-18-72(a)(4) (In Georgia, all investigatory records must remain closed until the pending subject matter is "concluded").

[32] *APCO Report, supra* note 5, at 7-8.

[33] *APCO Report, supra* note 5, at 12-18.

from making specific suggestions for municipalities, cities, and states that wish to deploy NG911 data collection and storage systems. These are choices are a balancing act between transparency and public safety that each division of government will have to determine based on an understanding of their own circumstances and community of stakeholders.

D. Compliance Mechanisms and Remedy Considerations

In a NG911 world, a custodian of public safety response records, with the assistance of qualified counsel, will be in a difficult position to evaluate what is and what is not subject to disclosure. If a custodian of the records fails to disclose information that should have been disclosed underneath the ORL, remedies range from state to state, but are relatively light in a single instance of non-compliance.[34]

Some commentators argue there is little incentive for state record holders to comply with the statues obligations because there is inconsistent treatment for violations.[35] Currently, nearly 90% of challenged denials are upheld by local courts.[36] However there is a real possibility that increase in the size and scope of data collected by NG911 systems will complicate the analysis further complicating the ORL compliance administration for state record holders.[37]

The penalties for wrongfully denying inspection rights to a qualified requestor vary greatly from state to state.[38] They typically fall in four categories: injunctive relief, criminal penalties, civil penalties, and punitive damages.

Thirteen states grant requesters the right to petition for a writ of mandamus compelling a holder of a requested record to turn over the document in extraordinary circumstances and/or declaratory judgements for future similar cases.[39] Unlike a writ of mandamus, a declaratory judgement only establishes that a right of inspection exists rather than a compensatory obligation to turn over the document requested.[40] A small group of states allow requesters to ask for sanctions against individuals who fail to comply with the state statue though these statues are much more rare.[41]

Many states allow for criminal penalties for the individuals who wrongfully deny inspection rights. Fourteen states impose criminal fines, and sixteen states allow for up to a year in jail for a

---

[34] *See* Margaret Kwoka, *Deferring to Secrecy*, 54 B. C. L. Rev. 185, 208 (2013).
[35] *Id*; *see also* Prime, *supra* note 22, at 353.
[36] Prime, *supra* note 22, at 361
[37] *Id.* at 210.
[38] *See* Daxton R. Stewart, *Let Sunshine in, or else: An Examination of the "Teeth" of State and Federal Open Meetings and Open Records Laws*, 15 Comm. L. & Pol'y 265 at 267 (2010).
[39] *E.g.,* D.C. Code Ann. § 2-537(a)(1).
[40] Stewart, *supra* note 37, at 268
[41] *Id* at 271 (eight jurisdictions allow for disciplinary action against the individual who improperly denies a right of inspection; Florida, Iowa, Maryland, Minnesota, Missouri, Nebraska, Vermont, and Federal FOIA.).
(continued…)

violation.[42] Though these penalties seem harsh in the abstract, many commentators note that they are rarely enforced.[43]

Civil penalties range significantly between states who impose them but generally fall into two categories; reasonable attorney's fees and compensatory damages.[44] Only a few states do not allow for the payment of reasonable attorney's fees for an ORL violation.[45] A handful of states allow for compensatory damages, charging $100 per day if the denial of inspection was unreasonable.[46]

Few states have imposed punitive damages against an agency that failed to disclose information subject to the open records act.[47] Only three states have statutorily allowed for punitive damages, though at least five more states are contemplating legislation that would allow for these damages to be assessed against a violating agency.[48]

If denial of inspection rights to those who request NG911 records occur on the basis that it would be unreasonable to redact or segregate protected information from disclosable information, an agency may be sued for discriminatory practices with severe consequences.[49] For example, fifteen states allow for treble damages when a custodian willfully denies inspection rights.[50] Furthermore, a few of these states have demonstrated their willingness to impose large compensatory fines, and criminal fines if the states statues allow.[51]

As a result, public safety entities need to recognize and strike a delicate balance between public safety, personal privacy, and government transparency. State governments who wish to deploy NG911 data collection systems should consider the architecture of these systems before deployment, and how they will enable (or disable) the transparency administrations established in state ORLs, and what penalties will be handed down for non-compliance in their state.

III. PRIVACY

The architecture used by NG911 systems to store data will likely change how NG911 PSAPs navigate existing privacy laws. Organizing and storing data based on information type presents

---

[42] *See* Stewart, *supra* note 37.

[43] *Id.*

[44] *See, e.g.,* Colo. Rev. Stat. § 24-72-204(5); *see also* Justin Cox, *Maximizing Information's Freedom: The Nuts, Bolts, and Levers of FOIA*, 13 N.Y. City L. Rev. 387, 388-89 (2010).

[45] Stewart, *supra* note 37, at 200.

[46] *E.g.,* Wash. Rev. Code Ann. § 42.56.550(4).

[47] Iowa Code § 22.17(A)(19).

[48] *See* Mich. Stat. Ann. § 13.08(1); Wis. Stat. Ann. § 19.37(3); MD. Code Ann. § 10-623; *see also* Kate Ferguson, *Compliance Conundrum: The Use of Punitive Damage Provisions In State Freedom of Information Statues*, 46 Colum. Hum. Rts. L. Rev. 371, 402 (2014).

[49] Stewart, *supra* note 37, at 280.

[50] *Id.*

[51] Lindell v. City of Mercer Island, 833 F.Supp.2d 1276 (Dist. Ct. Wash. 2011) (awarding over $90,000 in compensatory damages for failing to turn over documents relating to a sexual harassment investigation, email records, and calendars by a former harassed employee).

(continued…)

advantages for limiting unintended disclosure of private material, such as recordings or confidential healthcare data, but may increase the difficulty of complying with state laws for data protection standards and data breach disclosures. When implementing NG911 systems, stakeholders may want to take into consideration the interaction between system architecture, privacy concerns, and compliance with privacy laws.

The following sections will discuss potential challenges for NG911 related data from HIPAA, state recording laws, and data security and data breach requirements in the context of the centralized and decentralized visions of the systems.

A. Health Insurance Portability and Accountability Act (HIPAA)

The Health Insurance Portability and Accountability Act (HIPAA) is a comprehensive federal healthcare privacy law that places restrictions on disclosure of "protected healthcare information" ("PHI"), imposes security and storage requirements for entities that come into possession of PHI, and creates stiff penalties for violations of the HIPAA Privacy and Security Rules.[52]

HIPAA is relevant to NG911 because PSAPs and emergency personnel routinely come into contact with PHI and healthcare-related emergencies. NG911 will increase the amount of instances involving HIPAA and PHI by introducing even more confidential information into the 911 system.

Under current federal law, PSAPs are not bound by any HIPAA requirements as they do not qualify as a covered entity. HIPAA's requirements apply only to "covered entities," which are limited to "Health Plans," "Clearinghouses," and "Providers," as well as narrowly-defined "business associates" of covered entities.[53]

Despite PSAPs themselves not being bound by HIPAA requirements, HIPAA still presents issues when PSAPs must interact with other organizations that are covered entities, such as hospitals, health insurance companies, or other healthcare providers. For example, these covered entities are bound by HIPAA restrictions on disclosure of PHI, meaning that PSAPs will need to articulate an exemption in HIPAA in order to obtain PHI from any covered entity.[54]

HIPAA contains several exemptions that allow release of PHI for public safety and law enforcement purposes.[55] The two exemptions that are most applicable to NG911 are 45 C.F.R. §§ 164.512 (f)(3) and (j)(1)(i). The (f)(3) exemption allows for release of PHI when the individual whose information is to be released has been the victim of a crime.[56] Information may be released with direct consent, or without consent if the individual is incapacitated or incapable of providing consent due to some emergency condition.

Under (j)(1)(i), covered entities may release information if the covered entity believes, in good faith, that disclosure is necessary to prevent or lessen a serious and imminent threat to the health or

---

[52] 45 C.F.R. §§ 160, 162, 164.

[53] *Covered Entities and Business Associates*, DEP'T OF HEALTH & HUMAN SERVICES, http://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html (last visited Dec. 20, 2017); 45 C.F.R. § 160.102.

[54] 45 C.F.R. § 160.103.

[55] *Id.*

[56] 45 C.F.R. § 164.512 (f)(3).

(continued…)

safety of a person, and the information is being provided to someone reasonably able to prevent or lessen the threat.[57]

Using either exemption, PSAPs could theoretically obtain PHI to provide to law enforcement and emergency medical personnel responding to emergency situations where someone has been the victim of a crime or requires immediate medical assistance. Disclosure of PHI remains at the discretion of the covered entity, meaning that some entities may still refuse to provide PHI to PSAPs.[58] Requiring mandatory reporting to PSAPs may facilitate easier access for PSAPs to PHI, but may also lead to impacts, such as imposition upon PSAPs of HIPAA Privacy Rule and/or Security Rule disclosure and protection requirements.

Another HIPAA-related issue involving PSAPs is security of PHI. PSAPs are not covered entities, and thus are not required to comply with the HIPAA Security Rule requirements for PHI storage or HIPAA requirements for disclosure of PHI to third-parties.[59] Additionally, because NG911 PSAPs would not fall into any "covered entity" category, they would also not face any of the statutory fines or criminal penalties imposed directly by HIPAA if they were to improperly disclose or fail to secure PHI.[60] However, PSAPs might still be penalized under applicable state healthcare or privacy laws, and could face considerable civil liability through lawsuits in the event of an improper disclosure or data security failure.[61]

B. State Recording Laws

Many states have enacted laws regulating the recording of individuals, particularly with regard to private conversations or other private interactions. These laws may hamper the implementation of certain NG911 functionalities, such as the ability of PSAPs to receive streaming of live, multimedia content. New NG911 multimedia technologies will inevitably create obstacles when private conversations or interactions are recorded without consent of one or more parties involved. Enabling PSAPs to receive live video and audio from 911 callers, crash notification systems, or other sources could bring PSAPs into conflict with state recording laws, as individuals who are audio-recorded may not have provided consent necessary to make the recording legal. This could lead to potential evidence being deemed inadmissible in court, as well as fines against the recording entity and/or the PSAP receiving or storing the recording.

As an example, consider automatic crash response technologies, telematics services such as OnStar or LexusLink, which are already in use in many vehicles. These systems are currently capable of transmitting audio to a monitoring company but could potentially be used to transmit live audio and video directly to a PSAP, public safety data analytics center, or other emergency response entity for a faster and more efficient emergency response.[62]

For example, vehicles in the aforementioned multicar pileup example could be equipped with automatic crash response technology. With NG911, this technology could be connected directly

[57] 45 C.F.R. § 164.512 (j)(1)(i).
[58] 45 C.F.R. § 164.512.
[59] 45 C.F.R. § 160.103; 164.302.
[60] 45 C.F.R. § 160.300 – 160.400.
[61] Cal. Health & Safety Code § 1340 *et. seq.*
[62] *APCO Report, supra* note 5, at 10.

with a NG911 PSAP, enabling NG911 telecommunicators to speak directly with vehicle occupants, view live video of the interior and exterior of the vehicle, and record the incident for open records and other legal compliance requirements.

Immediately after the collision, the vehicles' automatic crash response systems could begin transmitting video and audio directly to a PSAP, where recording begins. The occupants of the vehicles are not informed that they are being recorded, nor is any express consent provided. Unaware that she is being recorded and before being contacted directly by a 911 telecommunicator at the PSAP, one of the drivers makes a self-incriminating statement to a passenger in her vehicle acknowledging fault for the accident. Though these concerns could likely be alleviated through a provider's terms of service and recording in the event of an emergency, there are still concerns that this could be seen as an unauthorized access to the content of a communication.[63]

State recording laws are divided into two types: single-party and two-party consent.[64] In a single-party consent state, only one party to a conversation or interaction must provide consent for a recording to be legal, and there are generally no requirements for disclosure of the recording activity to other parties to the conversation. In a single-party consent state, a 911 telecommunicator can provide the sole consent necessary for a 911 interaction to be recorded. Other states have adopted two-party consent laws that require consent to be obtained from all parties involved in the conversation or interaction.

Under the legacy system, a 911 telecommunicator can provide the consent necessary to allow recording in a single-party consent state. Two-party consent states have either adopted an implied consent doctrine or enacted emergency exemptions to allow recording without express consent from the caller.[65]

While some state recording laws may already contain exemptions for recording restrictions during emergency situations, some laws may not exempt emergency recordings, or may create potential liability due to ambiguity in the law.[66] The penalties for violations of state recording laws can be quite severe, with violations often labeled as felonies involving substantial fines and jail time. It is unclear how these penalties would impact state government employees beyond exclusion of any unlawfully obtained evidence from use in a criminal proceeding.

---

[63] *See* 18 U.S.C. §2511(2)(Most states recording laws are modeled after the Wiretap Act, including their exceptions. The "consent" and "color of law" exceptions would likely relieve a PSAP or government agency from liability if the service provider had a disclosure within their terms of service. This is a contractual law question that is outside the scope of this analysis).

[64] *Recording Phone Calls and Conversations*, DIGITAL MEDIA LAW PROJECT, http://www.dmlp.org/legal-guide/recording-phone-calls-and-conversations (last visited Dec. 4, 2017).

[65] *Laws on Recording Conversations in All 50 States*, MATTHIESEN, WICKERT & LEHRER, S.C. (2017), https://www.mwl-law.com/resources/laws-recording-conversations-50-states/; Md. Code Ann., Cts. & Jud. Proc. § 10-402(C)(5) (2015); Mont. Code Ann. § 45-8-213(c)(i) (2015); Fla. Stat. § 934.03 (3)(g)(2) (2017); Conn. Gen. Stat. § 52-570d(b)(2) (2011); Tit. 18. Pa. Cons. Stat. § 5704(3); N.H. Rev. Stat. Ann. § 570-A:2 (h), (i) (2017).

[66] M.G.L. Ch. 272 § 99.

C. State Data Breach Laws

Many states have imposed additional statutes and regulations aimed at protecting private information from inadvertent disclosure or theft. These laws are relevant to NG911 because PSAPs operating at the state and local level may be required to comply with state data protection laws whenever they receive protected categories of information. For example, a PSAP in a state with general data protection requirements that routinely receives covered private information may have to comply with laws that impose comprehensive security requirements upon both public and private entities, including PSAPs.

State data breach laws relevant to NG911 include protections for specific types of information, standards for information security by public entities, and a requirement of data breach notices. Most state data breach laws are targeted toward the private sector, generally regulating businesses in the healthcare, financial, and telecommunications industries, and are often narrowly targeted and impose restrictions on specific regulated entities,. However, several states, such as California and Massachusetts, impose rather substantial requirements, including data protection standards and data breach notices, upon state (and sometimes local) agencies that collect and store any personal information on residents of their state.

California is also one of 48 states that have enacted data breach notice requirements on all private entities and state government agencies that handle personal information.[67] California's Civil Code Sections 1798.29 and 1798.82 were some of the first state-level requirements for data breach notice. Under these sections, any person, business, or state government agency that owns or licenses personal information must notify a California resident of any possible breach involving their information.[68]

California is not the only state that imposes specific data protection requirements and data breach notice requirements. Massachusetts General Laws, Chapter 93H imposes upon all private entities and public agencies (including local government entities), a duty to report any security breaches or unauthorized uses of personal information "as soon as practicable and without unreasonable delay."[69] Detailed information must be provided by the public agency, including the date or approximate date of the breach and any steps taken by the agency in relation to the breach.[70] Unlike the California law, the Massachusetts law is not restricted to state agencies and would impact NG911 regardless of system architecture if data security is breached.[71]

Additionally, as NG911 functionalities allow PSAPs to receive and store an ever-increasing amount and variety of private information, states such as California may alter their laws to bring even local PSAPs into the fold of regulation, making compliance with data protection and data breach notice laws necessary, more difficult, and more important for PSAPs.

---

[67] *Security Breach Notification Laws*, NCSL (Mar. 29, 2018), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.
[68] Cal. Civil Code § 1798.29(a); § 1798.82(a).
[69] M.G.L. ch.93H § 1(a); § 3(a); § 3(b).
[70] M.G.L. ch.93H § 3(a).
[71] M.G.L. ch.93H § 1(a).

D. Architecture Considerations Related to Privacy

Under the centralized NG911 model, the PSAP will function as a hub through which all data and information must pass before being organized and distributed to the applicable emergency responders. PSAPs will now have access to a great deal of protected privacy information and it is still unclear what obligations the PSAP will have in protecting that information. If this information is collected, stored, and disclosed pursuant to ORLs at a local public safety data analytics center, that center may incur additional obligations to protect that information which has not previously been contemplated by NG911 systems.

Legacy 911 systems that are currently being utilized are more decentralized, meaning that PHI may be in the custody of emergency response agencies themselves, such as public or private ambulances, that may or may not be affiliated directly with a hospital. A hospital is covered entity under HIPAA, making hospitals liable for HIPAA penalties and data protection requirements.[72] Private ambulance companies affiliated with hospitals may also be covered by HIPAA as either an extension of the hospital itself, or as a "business associate" to a covered entity.[73] If the PSAP is gaining access to this data and storing it in some way in behalf of the first responders and the hospitals, there may need to be a reevaluation of the PSAPs status for protecting personal health information of individuals involved in emergency responses.

When considering HIPAA disclosure and security requirements, it is important to remember that HIPAA does not supersede stricter state laws.[74] HIPAA functions as a floor rather than a ceiling, meaning that states may impose additional and more stringent requirements.[75] PSAPs must ensure they are compliant both with HIPAA and any applicable state healthcare and privacy laws.

A centralized environment may also impact state recording and wiretap laws. If all NG911 response data (including voice data, telemetry data, multimedia files, utility maps, health data, etc.) could be combined into one file, there are some interesting dynamics of how that includes all the content comprising the "call." This approach could potentially create more disclosable content for public consumption, but is more likely to result in disclosure of private or protected information.

Finally, state data breach laws could potentially complicate NG911 data collections and storage implementation. Storing all data related to a call as one file could be beneficial from a standpoint of legal compliance, as the storing entity would be able to more easily comply with data protection laws. As an example, the California Information Practices Act requires state agencies to maintain a record of where data originated from.[76] If all data related to a call is stored as one file, the storing entity could simply maintain a single record stating that the data originated from, for example, "911 call from phone number 123.123.1234 at 10:30 A.M. on 1/1/2020."

---

[72] *Covered Entities and Business Associates*, *supra* note 50.
[73] *Id.*
[74] 45 C.F.R. § 160.203(b).
[75] *Does the HIPAA Privacy Rule preempt state laws?*, DEP'T OF HEALTH & HUMAN SERVICES, https://www.hhs.gov/hipaa/for-professionals/faq/399/does-hipaa-preempt-state-laws/index.html (last visited Apr. 29, 2017).
[76] Cal. Civil Code § 1798.16(a).

Under the decentralized NG911 model, data collection and storage where the discrete pieces of data are collected and stored separately and possibly by separate entities, some of the HIPAA privacy concerns are diminished. Storing HIPAA and other healthcare information separately from other data could reduce potential liabilities under both HIPAA and state healthcare privacy laws. If protected data such as PHI is stored separately from other data, the entity responsible for overseeing the data could potentially help ensure that certain categories of information are not improperly disclosed and that proper security measures are taken based on the type of data and the laws surrounding it.

Separating a multimedia NG911 "call" into different files, for example separate audio and video, is one potential approach that may make compliance with open records laws easier, as a PSAP could then work within the statutory framework to determine which constituent parts of the call are subject to disclosure.[77] However, separating a call into multiple files may result in less information becoming publicly available, increase administrative costs, and concerns for transparency advocates.

Data breach concerns are a mixed bag of benefits and concerns when considering the privacy implications of a decentralized deployment of NG911. First, a decentralized version of NG911 data management has the benefit of decreasing the amount of potential information that might be taken or lost in a data breach.[78] Some researchers suggest that holding information in different locations or mitigating the amount of information that can be lost decreases the potential cost of a data breach.[79] If NG911 data management systems can effectively distribute information effectively, it could potentially decrease the value of the information that could be gained in a data breach.

However, depending on how the system is architected, this distributing information may also have the unintended consequence of increasing the vectors of attack for a potential data breach. Attack vectors are potential paths or vulnerabilities in a system that attackers can use to access protected information.[80] As systems become more complex, there is an increase in the number of vectors of attack and a greater need for more robust cybersecurity efforts to protect sensitive information that reside within those systems.[81]

---

[77] *See* discussion *infra* Section II.A.

[78] *2017 Cost of Data Breach Study: Global Overview* 17, PONEMON INSTITUTE (2017), https://www-01.ibm.com/marketing/iwm/dre/signup?source=urx-15763&S_PKG=ov58441.

[79] Pratyusa K. Manadhata & Jeanette M. Wing, *An Attack Surface Metric*, 37 IEEE Transactions on Software Eng'g 371 (2008).

[80] Paul Cichonski et al., *Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology*, NIST (2007), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf.

[81] *Framework for Improving Critical Infrastructure Cybersecurity*, NIST (Dec. 5, 2017), https://www.nist.gov/sites/default/files/documents/2017/12/05/draft-2_framework-v1-1_without-markup.pdf.

IV. CHAIN OF CUSTODY

The data collected by NG911 systems carries not only public and private interest, but investigatory interest. This investigatory interest will amplify the complexity of questions around chain of custody and data retention requirements for that data. When NG911-enabled PSAPs or other public safety entities receive text messages, video calls, social media posts, medical information, and surveillance data, questions will arise regarding how traditional chain of custody rules and laws will apply. Additionally, whether NG911 data is stored in a centralized location such as a PSAP, or if different entities house certain types of data will likely give rise to an issue of compliance with chain of custody procedures.

This section outlines the applicable rules of evidence for authenticating or identifying evidence and how the examples of this rule could be satisfied by public safety entities as they implement NG911 technology. We then set forth some of the technological challenges that PSAPs and other public safety entities will likely encounter as they continue to implement NG911 data systems infrastructure, and how these issues will likely impact chain of custody procedures. Finally, this section lays out potential solutions and controls for how public safety entities may properly handle NG911 data in order to adequately comply with chain of custody procedures.

A. Chain of Custody and Federal Rules of Evidence

Chain of custody is traditionally defined as the movement and location of physical evidence from the time it is obtained until the time it is presented in court.[82] For chain of custody in federal court, the Federal Rules of Evidence provide a framework for authenticating or identifying evidence. It is important to note that evidence rules at the state level are heavily modeled after the Federal Rules of Evidence.[83] Therefore, this section focuses on how evidence rules at the federal level apply to NG911 systems and technology.

Specifically, Rule 901(a), Authenticating or Identifying Evidence, states: "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."[84] In essence, this means that the individual advocating in court for the use of certain evidence has to be able to sufficiently verify the integrity of that particular piece of evidence.[85]

Rule 901(b), sets forth some examples considered sufficient for evidence authentication. Specifically, Evidence About a Process or System, Rule 901(b)(9), is the most important example pertaining to NG911 data management and complying with chain of custody procedures.[86] Under this rule, there is a requirement for evidence to demonstrate the sufficiency of the process that

---

[82] Mike Byrd, *Proper Tagging and Labeling of Evidence for Later Identification*, CRIME SCENE INVESTIGATOR NETWORK, http://www.crime-scene-investigator.net/tagging.html (last visited Dec. 9, 2017).
[83] *See generally* Fed. R. Evid. 901; *see also* John Bourdeau et. al, *Adoption of Federal Rules by State*, 12 Fed. Proc., L. Ed. § 33:4 (2017).
[84] Fed. R. Evid. 901.
[85] *Id.*
[86] *Id.*
(continued…)

"produces an accurate result" and a requirement for a demonstration of how of the process functions.[87]

In applying Rule 901 to NG911 data, it is likely that offsite data storage companies, or PSAP IT administrators may be subject to testifying in court as to the process of NG911 data compilation and storage, along with how the integrity of the data is maintained. In essence, this testimony will likely be crucial to ensure that any NG911 data will be admissible in legal proceedings. One problem that might arise from validating the processes of offsite storage is that offsite data storage companies may be unsure as to what data is being stored on their systems.[88]

A second provision relevant to NG911 data is Rule 901(b)(1), Testimony of Witness with Knowledge, which says that a party must provide "testimony that an item is what it is claimed to be."[89] Currently, PSAP personnel within a legacy 911 system only possess audio recordings and limited amounts of data, such as the incident record, radio traffic recordings, responding agency reports, to confirm from an evidentiary perspective.[90] With NG911, significant and highly technical data pertaining to hardware, applications, and services will be available, and most 911 personnel may not have the technical expertise to testify; though courts have generally give deference to law enforcement entities that collect digital evidence.[91] Moreover, this example could suggest that a witness in a criminal case may have to testify as to the validity or integrity of a piece of digital evidence that was forwarded to the PSAP, such as a text message, video, social media posting, or possibly health information. Additionally, an expert witness may be required to help the court understand details about the electronic evidence. It is foreseeable that testimony from 911 personnel or individual submitters of different types of NG911 data will be essential for verifying and authenticating the data the PSAP has collected.

A third example pertaining to NG911 technology is Rule 901(b)(5), Opinion About a Voice, which is "an opinion identifying a person's voice—whether heard firsthand or through mechanical or electronic transmission or recording—based on hearing the voice at any time under circumstances that connect it with the alleged speaker."[92] Traditionally, this rule has been applied to the identification of voice in simple telephone conversations. However, this form of voice identification is not outside the realm of being applicable to NG911 technology. For example, an emergency call might beplaced from a VOIP phone, an OTT application, a video call, or a social media video with audio content that was part of an investigation. The NG911 technology that

---

[87] *Id.*

[88] *See generally* Pauline C. Reich, *Cybercrime & Security* § 2.4, THOMSON REUTERS (2012), http://www.academia.edu/2115230/Cybercrime_and_Security (discussing best practices for storing digital evidence and the difficulties with third-party vendors).

[89] *Id.*

[90] *Text 911 Master PSAP Registry, supra* note 16 (only a few states have begun to move beyond traditional services, but there is greater movement toward E-911 services).

[91] *See* VIRGINIA V. SHUE & JAMES S. VERGARI, FUNDAMENTALS OF COMPUTER-HIGH TECHNOLOGY LAW (1991).

[92] Fed. R. Evid. 901(b)(5).

(continued…)

collects voice data would then, in a legal scenario, require an opinion by someone on the call or who listened to a recording, to identify the voice at issue in order to satisfy this Rule.

In relation to the previous Rule on an opinion about a voice, the next example is Rule 901(b)(6), Evidence About a Telephone Conversation.[93] Here, there must be evidence for telephone conversations that:

> A call was made to the number assigned at the time to (A) a particular person, if circumstances, including self-identification, show that the person answering was the one called; or (B) a particular business, if the call was made to a business and the call related to business reasonably transacted over the telephone.[94]

This could be relevant to the NG911 PSAP because in addition to telephone calls, text messages and video calls made to a PSAP may be subject to these self-identification and verification requirements. It is foreseeable that courts may require a validation of the form of communication made to an assigned number or device of a specific person or business that may have submitted data other than a standard telephone conversation to a PSAP. For example, validating a text message may involve obtaining records from a wireless carrier, or testimony of receipt of a text message from an individual submitter and PSAP employee, in order to validate the time stamps and individuals who are corresponding. Essentially, there may have to be an additional validation for the other means of communication utilized in NG911 technology.

Also, Evidence About Public Records, Rule 901(b)(7), may have relevance to PSAP record keeping and chain of custody compliance for NG911. Under Rule 901(b)(7), there must be "evidence that: (A) a document was recorded or filed in a public office as authorized by law; or (B) a purported public record or statement is from the office where items of this kind are kept."[95] It is possible that data compilations or digital records compiled from NG911 could constitute a "record or statement" under this rule.[96] This is because records are now often kept digitally and in a PSAP, records could comprise of NG911 aggregated data from an incident. Therefore, in a legal environment, these digital records would need to be validated by the PSAP, or the entity that is responsible for the storage of the data, so they can be admitted into evidence.

B. Architecture Considerations

Just as with physical evidence, it is essential that public safety entities maintain a clear, documented chain of custody that would normally be present with traditional evidence. From the moment any type of NG911 data is obtained, a trail must document how it has been handled, by whom, and for what purpose.[97] While these evidentiary requirements have been traditionally applied to legacy 911 call recordings, the complex variety of data gathered by NG911 will create new

---

[93] *Id.*

[94] *Id.*

[95] *Id.*

[96] *Id.*

[97] Fed. R. Evid. 901.

(continued…)

challenges, including how the different forms of digital data will be stored, exchanged, logged, and secured, so as to comply with chain of custody procedures.

PSAPs storing NG911 data, whether on or offsite, must first consider the possibility of tampering. This issue is prevalent when evidence must be signed in or out to establish chain of custody, but because the evidence is digital, it is at risk to being tampered with.[98] To elaborate on the risk, NG911 data may include video, electronic documents, or photos, which could be subject to tampering in situations where digital evidence is being sent to multiple parties, through unauthorized access into a PSAP's server, or the through the modification of documents such as email prior to trial.[99] Moreover, PSAPs migrating their infrastructure to store more digital forms of evidence for NG911 systems may face greater procedural challenges, such as how evidence is routinely checked in and out for chain of custody purposes.[100]

Additional chain of custody issues may arise where NG911 systems utilize cloud or offsite storage.[101] NG911 systems may be implemented in a way that leave third-party vendors possessing, encrypting, and transmitting evidentiary data, which in turn could lead to challenges of the sufficiency and integrity of the evidence.[102] Furthermore, because the digital evidence might be possessed by a third-party, governmental entities will be tasked with proving the chain of custody is secure when presenting the data in court.[103]A variation of state laws pertaining to evidence retention or offsite storage could potentially give rise to a choice of law, as well as venue issues.

A third concern involves the consolidation of different types of data from NG911 platforms, whether at a centralized PSAP, or shared among different entities. With the various forms of data stored through NG911 processes, there potentially lies both a privacy and evidentiary matter with the aggregation of data that is being created.

A final point is that chain of custody is a human driven process in which the transfer of evidence depends on people handling the physical evidence properly. Essentially, this process is prone to human error and mistakes are inevitable.[104] It is foreseeable that employees at various

---

[98] *Authenticating Digital Evidence – Identify and Avoid the Weak Links in Your Chain of Custody*, MERRILL LEGAL SOLUTIONS, https://www.criminallawlibraryblog.com/wp-content/uploads/sites/335/2016/09/Authenticated_DigitalEvidence_2-20-09.pdf (last visited Dec. 9, 2017) [hereinafter *Authenticating Digital Evidence*].

[99] *See Id.* Adam Stone, *Chain of Custody: How to Ensure Digital Evidence Stands Up In Court,* GOVTECHWORKS (Sep. 17, 2015), https://www.govtechworks.com/chain-of-custody-how-to-ensure-digital-evidence-stands-up-in-court.; Keith G. Chval, *How to Preserve Digital Evidence in Case of Legal Investigation,* EDTECH (Oct. 31, 2006), https://edtechmagazine.com/higher/article/2006/10/how-preserve-digital-evidence-case-legal-investigation.

[100] *Id.*

[101] Chval, *supra* note 95.

[102] *Id.*

[103] *Id.*

[104] *Id.*

(continued…)

public safety entities handling and managing the electronically stored data may give rise to errors such as forgetting to log a piece of evidentiary data, not encrypting a file, or the occurrence of a data breach.[105] Another factor to consider is keeping all law enforcement, legal, and technical employees informed of technological upgrades and implementation of new NG911 capabilities, with emphasis on maintaining proper procedures to ensure chain of custody compliance for data.[106] There will likely be genuine concern over how each type of employee is trained or informed about changes to NG911 systems, impacting evidentiary procedures and potentially leading to significant impacts on a pending matter involving the validation of data.[107]

C. Opportunities for Enhanced Data Management

Several methods have been identified that may aid in ensuring compliance of chain of custody procedures for digital evidence. Some PSAPs have already implemented facets of the NG911 system, such as text-to-911, and are utilizing some of these methods[108]; however, there are many PSAPs, especially those in rural communities, that are just beginning to discuss these issues as they ponder implementation. It is crucial to keep in mind the two different scenarios of data storage architecture, with one being the PSAP acting as a public safety data analytics center for all data, or different types of NG911 data being stored among different entities. The architecture of storage is relevant because it may impact the degree of difficulty in how these solutions are implemented in a NG911 context.

A potential method of compliance for ensuring data integrity pertaining to chain of custody is digital hashing using specialized software. Hashing is a digital fingerprint of the digital evidence, which "uses an algorithm to create a unique digital impression of a digital record. Any change to that record afterward will result in a new, unique hash."[109] A common example used is with a digital photo, where if one pixel were altered it would change the entire hash.[110] Using hashing for digital evidence would likely help alleviate concerns over third-party storage due to the authentication methods, and act as a major deterrent to those who wish to engage in tampering.

Specialized software exists that allows for the seamless copying of data that could also be used to ensure integrity.[111] This software could be either a form of forensic collection software or an appliance that could retrieve electronically stored information (ESI) from networks and devices

---

[105] *See id.*

[106] *Next Generation 9-1-1 Transition Policy Implementation Handbook*, NENA (Mar. 2010), http://www.nena.org/resource/resmgr/ngpp/ng911_transition_policy_impl.pdf?hhSearchTerms=%22ng911+and+transition+and+policy%22.

[107] *See id.*

[108] *PSAP Text-to-911 Readiness and Certification Form*, FCC, https://www.fcc.gov/general/psap-text-911-readiness-and-certification-form (last visited Feb. 28, 2018).

[109] Stone, *supra* note 95; Stephen Northcutt, *Security Laboratory: Cryptography in Business Series*, SANS TECHNOLOGY INSTITUTE, https://www.sans.edu/cyber-research/security-laboratory/article/hash-functions (last visited Dec. 9, 2017).

[110] *Id.*

[111] *See* Chval, *supra* note 95.

(continued…)

while ensuring integrity of the data.[112] The issue of metadata integrity may also arise during the copying process, which provides "basic information about data, such as type of asset, author, date created, usage, and file size . . . [and] is crucial to the efficiency of information systems to classify and categorize data.[113] The copying process could be especially relevant for NG911 data repositories because a PSAP may have to authenticate metadata off a hard drive when evidence is signed in and out from a data repository.[114] When data is copied or moved, an "electronic fingerprint" can also be utilized to ensure the integrity of the data as it is moved and accessed.[115]

Collaboration between all groups involved in the chain of custody procedures is critical for authentication. PSAPs should institute a working procedure for collaboration between the IT staff responsible for the data storage, the legal team, and law enforcement.[116] Furthermore, it is recommended by some data storage and security professionals that "a single third-party service provider collect and process the evidence to ensure standardized procedures are followed."[117] Then, if the collection procedure is challenged, a witness from the electronic evidence service provider can offer relevant testimony, ensuring that all the links in the chain of custody are intact, which will in turn make it easier to satisfy Rule 901(b)(9), Evidence About a Process or System.

Conclusion

NG911 technology is quickly being adopted across the country and there are questions that need to be addressed before a deployment rather than ad hoc. One specific question that state and local governments need to consider is how these systems are architected to comply with already existing legal obligations.

First, data collection and storage systems that are deployed in a very centralized way can be helpful for compliance with data breach laws and chain-of-custody evidentiary requirements, but could be a detriment to ORL compliance and HIPAA compliance. This monolithic version of a NG911 data management system is something that many industry groups and agencies think will be possible in the near to midterm future.

A centrally aggregated system with the PSAP acting as a public safety data analytics center for NG911 data would also aid in streamlining the evidentiary process for complying with procedures and validation. As discussed in Section IV, there are various concerns over how the public safety entities will store data to ensure adequate compliance with chain of custody procedures. Much of

---

[112] *Id.*

[113] Bernard Marr, *What Is Metadata? A Simple Guide to What Everyone Should Know*, DATA INFORMED (Apr. 10, 2017), http://data-informed.com/what-is-metadata-a-simple-guide-to-what-everyone-should-know/.

[114] *Authenticating Digital Evidence*, *supra* note 94; Chval, *supra* note 95.

[115] *Id.*

[116] *See* Karen Kent, Suzanne Chevalier, Tim Grance & Hung Dang, *Guide to Integrating Forensic Techniques into Incident Response*, NIST, http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf (last visited Dec. 9, 2017) (NIST also encourages similar cooperation through its guidelines as well).

[117] *Authenticating Digital Evidence*, *supra* note 94; Stone, *supra* note 95.

this concern will likely be alleviated with the PSAP being the public safety data analytics center, rather than having the data spread among the various entities. Specifically, with all the data being managed by the PSAP, it is foreseeable that the process for establishing evidentiary procedures can be streamlined in way where there can be adequate security and management, proper logging procedures for access, and a more efficient process for testifying in cases for authenticating the data.

Centralized storage will make it more difficult for open records custodians to identify exempted private information, such as HIPAA data or multimedia recordings, but will make compliance with state data protection standards and data breach notices much easier and less resource-intensive. Rather than ensuring compliance of multiple emergency response agencies with comprehensive data protection standards, locating all data within a public safety data analytics PSAP means that only one entity, the data analytics PSAP, will need to expend time, personnel, and other resources to guarantee compliance.

However, even with these benefits, systems that are highly centralized pose problems for state ORL compliance. As discussed in section II, records that are large in size and scope often times are difficult to deal with, as they can contain information that is both subject to ORLs and statutorily exempted from disclosure. If state and local governments have large data files that are not easily segregable, it will become increasingly burdensome to comply with open records requests, and there are potentially large penalties for entities that frequently violate these requirements

The second version of this technology is less centralized and more diffuse in its implementation than the first. This architecture can be highly beneficial for protecting private information and ORL compliance, but have negative consequences data breach laws, data protection requirements, and evidentiary obligations. The system could be architected in a way where all of the data that is collected is stored separately—perhaps by different entities, such as a PSAP and various first responders—or even if aggregated could be easily segregated into its constituent parts—e.g., audio recordings, telemetry data, health information, etc. In other words, the system could be architected in such a way that the data could be queried at a granular level.

Organizing and storing data in a decentralized manner presents advantages for limiting unintended disclosure of private material such as multimedia recordings or HIPAA data, but may increase the difficulty of complying with state data protection and data breach notice laws. Decentralized storage reduces the risk of releasing protected information, as the entity responsible for maintaining the information can more easily locate and identify specific types of data that may be private.

If multiple entities were responsible for storing different types of evidentiary data, it would create a more complex administration for chain of custody compliance. Multiple agencies and entities would have to create common procedures for dealing with digital evidence. Moreover, if the data were to be managed by multiple entities, then it may give rise to difficulties such as, multiple parties having to testify in court for validation, more risk of human error in the logging process, and potential integrity and security concerns over data being housed by multiple entities.

Systems that are decentralized where information is queried at a highly granular level are a better option in the context of ORLs. If discrete piece of information about a NG911 response are stored separately (e.g. video data is separated from crash telemetry data) such that each piece of data is treated as a separate record, compliance with ORLs will be much easier. It will be easier for a

custodian of the records to syphon through relatively small and granular pieces of information to determine if the record is disclosable or exempted from disclosure.

There are benefits and drawbacks to both of these architectures that governments need to consider if they intend to deploy this technology. Advocates and practitioners need to understand that after data is collected by the government in response to an emergency, the information that they collect will be highly scrutinized by the communities in which they serve. These NG911 data management systems need to strike a balance between public safety, personal privacy, the rule of law, and government transparency that is acceptable to all the stakeholders in the community.

Appendix: Summary of Architecture Considerations

Summary of Architecture Considerations		
	Centralized Data Collection	**Decentralized Data Collection**
State Open Records Laws • *Scope of record* • *Data contained in record* • *Disclosable* • *Exempted*	• All parts of the call are part of the record and not segregable • Massive files • Inability to pull out just one part of call data (e.g. radio transmission) • Administrative and data management inefficiencies and complexities	• Each part of the call record are segregable • Individual files • Ease of administrative processing • Treatment of each data set could be different and may or may not be disclosable and may or may not be exempted • May have higher administrative cost implications
Privacy • **HIPAA** • *State and Fed recording laws* • *Data Breach laws.*	• HIPAA compliance more difficult. • Fewer vectors of attack for data breach purposes therefore easier to protect. But higher amount of sensitive information in one location with greater impact if breach occurs	• HIPAA compliance easier. • More vectors of attack therefore harder to protect the data. But lower amount of sensitive information in one location with lower impact if breach occurs.
Chain of Custody Obligations • *Chain of Custody and Data Retention* • *Chain of Custody and Federal Rules of Evidence* • *Chain of Custody and Technical Challenges*	• Likely easier to comply with authentication if files are stored in a centralized location. • If centralized, then collaboration between 911 entities will likely be more efficient. • Likely initial challenges with authenticating how different forms of digital data will be stored, exchanged, logged, and secured.	• May be more difficult to authenticate individual files if they are located on servers housed by different entities. • Collaboration between 911 entities might be more difficult if data located across the different entities. • Likely more difficulty in validating offsite storage if multiple vendors and multiple 911 entities are a part of the procedural process. • Different state laws pertaining to evidence retention or offsite storage could potentially give rise to a choice of law and venue issues