

**LEGAL, POLICY AND ETHICAL ISSUES OF  
USING BIG DATA AND PREDICTIVE  
ANALYTICS IN NEXT GENERATION (NG)  
911 TO NOTIFY AND AID THE DISPATCH OF  
FIRST RESPONDERS**

*Elaine Seeman\**

*James E. Holloway\*\**

*James Kleckley\*\*\**

---

\* Associate Professor, Management Information Systems, Department of Management Information Systems, College of Business, East Carolina University, Greenville, North Carolina 27858. B.A., Indiana University of Pennsylvania, 1973; M.B.A., East Carolina University, 1997; Ph.D., Indiana State University, 2002.

\*\* Professor, Business Law, Department of Finance, College of Business, East Carolina University, Greenville, North Carolina 27858. B.S., North Carolina Agricultural and Technical State University, 1972; M.B.A., East Carolina University, 1984; J.D., University of North Carolina at Chapel Hill, 1983.

\*\*\* Director, Bureau of Business Research and Research Associate Professor of Finance, College of Business, East Carolina University, Greenville, North Carolina 27858, B.S., University of South Carolina, 1976; PhD, University of South Carolina, 1984.

We give a special thanks to Dr. Stan Eakins, Dean, College of Business, East Carolina University, for awarding Dr. Elaine Seeman a Summer Research Stipend in summer 2014 to conduct research on the use of Big Data and Predictive Analytics in providing Next Generation (NG) 911 services. We also give a special thanks to Professor Janine Hiller, Virginia Polytechnic Institute and State University, Blacksburg, Virginia, and Professor Tonia Hap Murphy, University of Notre Dame, Notre Dame, Indiana, for inviting the authors to present this article at the *Colloquium on Big Data and Predictive Analytics: Legal, Policy and Ethical Issues of Using Supplementary Data in Next Generation (NG) 911 to Notify and Aid the Dispatch of First Responders*, Pamplin College of Business, Virginia Polytechnic Institute and State University, Blacksburg, Virginia, June 2014.

## ABSTRACT

Next Generation (NG) 911 services are slowly replacing Enhanced (E) 911 services that provide mostly location and emergency call data. NG911 services include location, data and voice and nonvoice emergency calls that are accompanied by an increase in the volume, complexity and variety of call data. NG911 systems will supplement the emergency call data with additional data so that law enforcement, emergency medical and other first responders can more effectively and efficiently provide emergency services. Additional data include spatial, geographical, medical, personal, terrain, environmental, and other data. The collection and delivery of these data by telecommunications carriers and 911 service providers to Public Safety Answering Points (PSAPs) (911 emergency call centers) and first responders raise legal, ethical and public policy issues. The use of additional data and predictive uses raise new privacy, liability and other concerns for telecommunications carriers, 911 service providers, PSAPs and first responders. Current communications and 911 statutes provide immunity and other protection to 911 service providers, PSAPs and persons, and a federal communications privacy statute grants an exception to privacy requirements of telecommunications carriers. This immunity and exception may not always extend to the collection and delivery of additional data and their predictive uses. However, statutory and regulatory restrictions on the collection and delivery of additional data and predictive uses may not allow PSAPs and first responders to prevent or reduce deaths, personal injuries, and property losses.

## TABLE OF CONTENTS

I.	INTRODUCTION .....	549
II.	COLLECTION & USE OF 911 DATA TO NOTIFY & AID FIRST RESPONDERS .....	553
	A. 911 Data in the Context of Information Management & Analysis.....	554
	B. Additional Data to Notify & Aid First Responders ...	555
	C. Increase of 911 Data to Notify & Aid First Responders.....	556
III.	LEGAL & REGULATORY ISSUES REGARDING THE COLLECTION OF 911 CALL DATA .....	557
	A. Federal Communications Law Governing the	

<b>2015]</b>	<b>BIG DATA &amp; PREDICTIVE ANALYTICS</b>	<b>549</b>
	Collection of 911 Data .....	558
	B. Impact of Cost on Collection & Delivery of 911 Data to PSAPs .....	559
	C. Legal Issues Regarding Use & Privacy of 911 Data..	561
IV.	ETHICAL QUESTIONS REGARDING THE COLLECTION OF 911 CALL DATA .....	562
	A. Personal & Other Sensitive Data Delivered to PSAPs .....	562
	B. Use of Personal Data & Predictive Uses by PSAPs & First Responders .....	564
	C. Ethical & Moral Harm of Disclosing 911 Data .....	565
V.	PUBLIC POLICY CONCERNS REGARDING THE COLLECTION & DELIVERY OF DATA .....	566
	A. Privacy, Liability & Other Public Policy Concerns ...	566
	B. Limiting Liability of Telecommunications Carriers & Other Providers .....	568
	C. Limiting Liability of PSAPs & First Responders as Users .....	569
VI.	CONCLUSION .....	570

## I. INTRODUCTION

The availability of and access to more 911 emergency call<sup>1</sup> and other data<sup>2</sup> creates the need to examine the collection, management, and use of big data and predictive analytics by 911 emergency call centers and other public safety divisions to notify, inform and aid law enforcement, emergency medical, fire and rescue, and emergency management agencies.<sup>3</sup> The 911

---

<sup>1</sup> See 47 U.S.C. § 942(e)(4) (Supp. 2013) (stating emergency calls include “voice, text, or video and related data; and . . . nonhuman-initiated automatic event alerts, such as alarms, telematics, or sensor data, which may also include real-time voice, text, or video communications”).

<sup>2</sup> See NAT’L EMERGENCY NO. ASS’N (NENA), NENA STANDARD FOR NG9-1-1 ADDITIONAL DATA 10 (2009) [hereinafter NENA, ADDITIONAL DATA], *available at* [http://c.ymcdn.com/sites/www.nena.org/resource/collection/F2E0D66A-4824-418C-8670-3238D262B84A/NENA\\_71-001-v1\\_NG9-1-1\\_Additional\\_Data.pdf](http://c.ymcdn.com/sites/www.nena.org/resource/collection/F2E0D66A-4824-418C-8670-3238D262B84A/NENA_71-001-v1_NG9-1-1_Additional_Data.pdf) (“Additional Data is defined as data that is associated with a call, a caller or a location. This data may also be either additional data depending on when the data is accessed, with the call or once the call is received at the PSAP.”). In addition, “[a] call is a generic term meaning an interactive multimedia session or an unattended device event.” *Id.* Additional Data is also associated with a PSAP and may be acquired from external sources. *Id.*

<sup>3</sup> See Kate Crawford & Jason Schultz, *Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms*, 55 B.C. L. REV. 93, 96 (2014)

emergency call system began with landline or wireline telephones that allowed subscribers to describe their emergency situations and give their locations.<sup>4</sup> The wireless or mobile cellular telephones allowed subscribers to give the emergency situation and location.<sup>5</sup> Unlike the landline or wireline telephones that were at a fixed location, the wireless telephones were mobile. If wireless subscribers could not give their location, 911 emergency call centers or Public Safety Answering Points (PSAPs)<sup>6</sup> could not give the location of the subscribers to first responders who must provide emergency assistance or services.<sup>7</sup> This situation created the need for Enhanced (E) 911 services that would automatically deliver to PSAPs both location and telephone number of wireless and wireline subscribers.<sup>8</sup>

Wireless and wireline E911 services were quickly followed by an increase in personal digital communications devices that are capable of requesting emergency services using voice and non-

---

(“Big Data is a generalized, imprecise term that refers to the use of large data sets in data science and predictive analytics.”) (internal quotations omitted). Professors Crawford and Schultz state that Big Data includes three aspects. First, they assert “it refers to technology that maximizes computational power and algorithmic accuracy.” *Id.* Next, “it describes types of analyses that draw on a range of tools to clean and compare data.” *Id.* Finally, “it promotes the belief that large data sets generate results with greater truth, objectivity, and accuracy.” *Id.* Other authors and commentators have analyzed the impact of big data and analytics on privacy and other interests and rights. *See, e.g.*, Nancy J. King & V.T. Raja, *What Do They Really Know About Me in the Cloud? A Comparative Law Perspective on Protecting Privacy and Security of Sensitive Consumer Data*, 50 AM. BUS. L.J. 413, 413–16 (2013) (examining “whether new information privacy laws are needed to protect the privacy and security of sensitive consumer data stored in the cloud and to support the growth of the cloud computing industry”); Omer Tene & Jules Polonetsky, *Judged By The Tin Man: Individual Rights In The Age Of Big Data*, 11 J. TELECOMM. & HIGH TECH. L. 351, 351–52 (2013) (identifying “privacy and non-privacy risks of big data as well as directions for potential solutions”).

<sup>4</sup> *See* FED. COMM’NS COMM’N (FCC), LEGAL AND REGULATORY FRAMEWORK FOR NEXT GENERATION 911 SERVICES: REPORT TO CONGRESS AND RECOMMENDATIONS, 2013 WL 771885, at 4–5 (2013) [hereinafter FCC, LEGAL AND REGULATORY FRAMEWORK] (proposing and recommending a NG911 regulatory framework to provide NG911 services).

<sup>5</sup> *Id.* at 5–6.

<sup>6</sup> *See* 47 U.S.C. § 222(h)(4) (2012) (“[P]ublic safety answering point’ means a facility that has been designated to receive emergency calls and route them to emergency service personnel.”).

<sup>7</sup> *See* FCC, LEGAL AND REGULATORY FRAMEWORK, *supra* note 4, at 6 (discussing how “the mobility of wireless subscribers makes permanent street addresses unreliable as location indicators” and “real-time location information” is required to route and location wireless 911 calls).

<sup>8</sup> *Id.*

voice calls and data.<sup>9</sup> This capability creates the need for PSAPs to receive voice and non-voice calls,<sup>10</sup> and establishes the need for Next Generation (NG) 911 services.<sup>11</sup> NG911 services use Internet Protocol (IP) technology that permits the public to request emergency services by making voice and non-voice calls, using automatic calling systems and providing videos, photographs and data.<sup>12</sup> These kinds of emergency calls or notifications may include additional and complementary data<sup>13</sup> so that first responders or emergency services providers<sup>14</sup> can better respond to emergency situations and threats.<sup>15</sup> The additional

---

<sup>9</sup> *Id.*

<sup>10</sup> *See id.* (“For a PSAP request to be valid, the PSAP must be capable of receiving and utilizing the data elements associated with either E911 Phase I or Phase II service.”) (internal quotations omitted).

<sup>11</sup> *See id.* at 7 (explaining NG911 services and discussing the numerous advantages of NG911 compared to traditional 911 services).

<sup>12</sup> *Id.*

<sup>13</sup> NENA, ADDITIONAL DATA, *supra* note 2, at 6 (“Supportive data is used during the 9-1-1 call flow to provide proper routing instructions such as Vehicle Emergency Data Set (VEDS). Supplemental data is retrieved after the call reaches the PSAP or the responding emergency agency such as building data or medical records.”). NENA chose not to divide the data into two categories because the data was interchangeable and indistinguishable. *Id.*

<sup>14</sup> *See* 6 U.S.C. § 101(6) (2012) (“The term ‘emergency response providers’ includes Federal, State, and local governmental and nongovernmental emergency public safety, fire, law enforcement, emergency response, emergency medical (including hospital emergency facilities), and related personnel, agencies, and authorities.”). The ordinary meaning of a first responder is “a person (as a police officer or an EMT) who is among those responsible for going immediately to the scene of an accident or emergency to provide assistance.” *First Responder*, MERRIAM-WEBSTER.COM, <http://www.merriam-webster.com/dictionary/first%20responder> (last visited Apr. 17, 2015). First responder does not include a legal or regulatory definition but is casually used by government agencies to describe the government and nongovernmental agencies responding to emergency situations. NAT’L COOP. HIGHWAY RESEARCH PROGRAM, RESEARCH RESULTS DIGEST NO. 385, at 1 (2013), *available at* [http://onlinepubs.trb.org/onlinepubs/nchrp/nchrp\\_rrd\\_385.pdf](http://onlinepubs.trb.org/onlinepubs/nchrp/nchrp_rrd_385.pdf) (“The conclusion reached after examining federal law, regulations, and other federal executive branch documents is that there is no ‘definition’ of the term ‘first responder.’ The term has come to be used popularly or colloquially to refer to law enforcement, fire, and emergency medical personnel.”). Moreover, federal legislation explicitly states that Public Safety Answering Points (PSAPs) are first responders. *See* 47 U.S.C. § 1401(22)(F) (Supp. 2013) (“The term ‘Next Generation 9–1–1 services’ means an IP-based system comprised of hardware, software, data, and operational policies and procedures that . . . provides broadband service to *public safety answering points or other first responder entities.*”) (emphasis added).

<sup>15</sup> *See id.* § 1401(22)(C) (defining “Next Generation 9-1-1 services” to include “acquir[ing] and integrat[ing] additional emergency call data useful to call routing and handling”).

and complementary data increase the volume, complexity, and variety of voice and non-voice calls<sup>16</sup> that create big data<sup>17</sup> and opportunities for predictive analytics.<sup>18</sup> Emergency call data and predictive analytics will be useful to notify and aid first responders to analyze and identify threat situations, allocate resources and design methods and means of responding to emergency situations.

The collection and delivery of big data and predictive uses by telecommunications carriers, 911 service providers, Public Safety Answering Points (PSAPs) and first responders raise legal, ethical, and public policy issues. The introduction identifies and explains how NG911 services create big data and predictive uses that can improve the effectiveness and efficiency of PSAPs and first responders. Part II examines the nature of NG911 systems

---

<sup>16</sup> See NENA, ADDITIONAL DATA, *supra* note 2, at 10 (including call data that were used to route the call to the PSAP and retrieved after the call reaches the first responder).

<sup>17</sup> See NAT'L 911 PROGRAM, REVIEW OF NATIONWIDE 911 DATA COLLECTION 5 (2013), available at <http://www.911.gov/pdf/Current911DataCollection-072613.pdf> (explaining that "911 Operational Data" is composed partly of "[c]all volume statistics" which includes "wireline, cellular, Voice over Internet Protocol, [VoIP], multi-line telephone system [MLTS], telematics, [and] other"). However, the National 911 Program finds that public safety is embracing big data and predictive analytics, but 911 services are not embracing big data and predictive analytics to improve management and operations of nationwide 911 services and public safety. The National 911 Program recognizes that public and private sectors are collecting data to support 911 services that must notify and can aid first responders. "The National 911 Program and the National Emergency Number Association (NENA) both collect data to understand the status of 911 services across the country. The private sector, including companies such as Intrado and FirstWatch, also collect proprietary data associated with their efforts to support and serve the 911 industry." *Id.* at 3.

<sup>18</sup> See P'SHIP FOR PUB. SERV. & IBM CTR. FOR THE BUS. OF GOV'T, FROM DATA TO DECISIONS: THE POWER OF ANALYTICS 2 (2011) [hereinafter P'SHIP & IBM CTR.], available at <http://ourpublicservice.org/publications/download.php?id=83> ("[Analytics] is the extensive and systematic use of data, statistical and quantitative analysis and explanatory and predictive models to drive fact-based actions for effective management. [Analytics] is the process of turning data into meaningful information that program staff and agency leaders can use to make decisions."). Organizations and agencies must use tools and technologies to conduct analytics to turn data into usable information and predictive uses. Statistical and quantitative tools and analytical models that permit agencies and organizations to "glean information from their data vary widely in sophistication. State-of-the-art tools are likely to afford the most in-depth analysis of data, but progress also can be made using existing software programs, such as computer spreadsheets." *Id.* at 6. Moreover, agencies and organizations can start an analytic program by "using in-house systems and commonly available desktop software and grow their programs as they gain experience in performance management." *Id.*

**2015] BIG DATA & PREDICTIVE ANALYTICS 553**

and services and the increase in and use of additional and complementary data to aid PSAPs and first responders. Part III examines and identifies legal and regulatory issues involving the liability of 911 service providers and PSAPs, and the privacy obligations of telecommunications carriers to use and deliver emergency call and additional data for emergency services. Part IV examines and identifies ethical questions involving the collection and use of personal and other sensitive data by PSAPs and first responders. Part V identifies and examines public policy concerns involving privacy, liability and other issues that are not governed by federal and state statutes. The conclusion states that big data and predictive uses allow PSAPS and first responders to provide more effective and efficient emergency services but create legal, ethical and public policy issues that must be addressed by business organizations and federal and state policy-makers.

## II. COLLECTION & USE OF 911 DATA TO NOTIFY & AID FIRST RESPONDERS

PSAPs, telecommunication carriers and other 911 service providers will collect and use more 911 emergency call and additional data.<sup>19</sup> These data were not normally available to notify and aid first responders.<sup>20</sup> E911 and 911 calls included only voice call data that were location and telephone number data of subscribers requesting emergency services.<sup>21</sup> NG911 services deliver voice, text message, video, alarm and other data that can include personal, medical and other data and predictive uses, such as public threats and threatening behaviors.<sup>22</sup> Commercial 911 service providers must provide and use analytics and technology to analyze emergency call and additional data to provide predictive uses to PSAPs and first responders.<sup>23</sup> If state

---

<sup>19</sup> See NAT'L 911 PROGRAM, *supra* note 17, at 3 (discussing why “[d]ata collection is extremely valuable” and therefore will continue).

<sup>20</sup> See *id.* at 4–5 (explaining how implementation of NG911 services is in progress, or just beginning in some states).

<sup>21</sup> *Id.* at 4 & nn. 4–5.

<sup>22</sup> NENA, NG9-1-1 SYSTEM AND PSAP OPERATIONAL FEATURES AND CAPABILITIES REQUIREMENTS 17, 26 (2011) [hereinafter NENA, NG9-1-1 SYSTEM AND PSAP OPERATIONAL FEATURES], available at [http://c.ymcdn.com/sites/www.nena.org/resource/collection/2851C951-69FF-40F0-A6B8-36A714CB085D/NENA\\_57-750\\_NG9-1-1\\_System\\_and\\_PSAP\\_Operational\\_Features\\_and\\_Capabilities\\_Requirements.pdf](http://c.ymcdn.com/sites/www.nena.org/resource/collection/2851C951-69FF-40F0-A6B8-36A714CB085D/NENA_57-750_NG9-1-1_System_and_PSAP_Operational_Features_and_Capabilities_Requirements.pdf).

<sup>23</sup> NAT'L 911 PROGRAM, *supra* note 17, at 10 (discussing private companies

and local governmental resources are available to analyze these data, PSAPs and first responders may use emergency call and additional data to make predictive uses.<sup>24</sup>

A. *911 Data in the Context of Information Management & Analysis*

As stated above, NG911 services include voice calls, text messages, emails, photographs, alarm signals, sensor data, and telematics.<sup>25</sup> Information management plays essential roles in the operation and management of NG911 systems that must continue to provide location data and respond to voice calls.<sup>26</sup> The use of information management means that “[a]ddresses now will be pre-validated through [Location Information Server] (LIS).”<sup>27</sup> Emergency “calls will arrive at the PSAP with a civic address or coordinate attached, and the [Geographical Information Server] (GIS) data in the [Emergency Call Routing Function] (ECRF) will be used to route the call.”<sup>28</sup> NG911 systems include information management systems that route and deliver emergency call and location data.<sup>29</sup> These roles of information management demonstrate the collection, storage and use of emergency call data to create usable information to support emergency services.<sup>30</sup> The nonvoice emergency calls and additional data expand the roles of information management to support and supplement emergency services.<sup>31</sup>

---

such as Intrado and FirstWatch that also collect such data and help provide emergency services).

<sup>24</sup> *Id.*

<sup>25</sup> FCC, LEGAL AND REGULATORY FRAMEWORK, *supra* note 4, at 10–11.

<sup>26</sup> See L.R. KIMBALL, THE DATA DIFFERENCE IN NEXT GENERATION 9-1-1 SYSTEMS 2 (May 2010) (on file with author) (explaining that information systems are needed to operate the NG911 system in order to deliver the caller’s location and telephone number to the 911 emergency call center or Public Safety Answering Point (PSAP)).

<sup>27</sup> *Id.*

<sup>28</sup> *Id.* at 2–3.

<sup>29</sup> See NENA, NG911 SYSTEM AND PSAP OPERATIONAL FEATURES, *supra* note 22, at 30 (stating that “[t]he Call Detail Record shall at minimum contain: date(s), times, . . . [c]aller location[,]” and other data).

<sup>30</sup> *Id.* at 6–7.

<sup>31</sup> See *id.* (“Significant work is currently underway to enable the 9-1-1 system to transition from telephone-based voice only systems to a fully interoperable Internet Protocol (IP) based, multimedia Next Generation 9-1-1 (NG9-1-1) system capable of supporting a variety of different communications devices and protocols.”).

*B. Additional Data to Notify & Aid  
First Responders*

Other information management systems are external to the NG911 systems and collect and analyze additional data and provide information and predictive uses, such as medical and building data.<sup>32</sup> Additional data will be “associated with a call, a location, a caller and a PSAP.”<sup>33</sup> NG911 systems will permit emergency calls to look at other data sources that “assist in determining the appropriate call routing and handling.”<sup>34</sup> For example, the use of the Vehicle Emergency Data Set (VEDS) to route crash information (calls from vehicles) to the appropriate PSAP.<sup>35</sup> Although VEDS and other data will be used in an information management system to notify first responders, these data can be used to aid first responders after delivery of the emergency call.

PSAPs and other first responders can retrieve personal and public data to aid in delivering more effective and efficient emergency services.<sup>36</sup> Personal and public data will contain more information to respond to emergency situations. For example, the PSAP or first responders can collect medical and building records to aid first responder providing law enforcement, fire or other emergency services.<sup>37</sup> Moreover, “additional data elements within this document or available from an external data source may be used by PSAP management to establish business rules/policies for call handling and routing” to appropriate first responders.<sup>38</sup> The NG911 system structure must be “able to accommodate multiple . . . services and structures for the same call,”<sup>39</sup> and “PSAP management will need to ascertain what additional data will arrive with 9-1-1 calls.”<sup>40</sup> NG911 systems will have the capability to support and supplement notification and dispatch of first responders by providing and using spatial, geographical,

---

<sup>32</sup> *See id.* at 26 (discussing the collection of additional data such as “floor plans [and] medical records data”).

<sup>33</sup> NENA, ADDITIONAL DATA, *supra* note 2, at 6.

<sup>34</sup> *Id.*

<sup>35</sup> *Id.*

<sup>36</sup> *Id.*

<sup>37</sup> *See id.* (“Supplemental data is retrieved after the call reaches the PSAP or the responding emergency agency such as building data or medical records.”).

<sup>38</sup> *Id.*

<sup>39</sup> *Id.*

<sup>40</sup> *Id.*

medical, personal, terrain, environmental and other data.<sup>41</sup>

*C. Increase of 911 Data to Notify  
& Aid First Responders*

NG911 call systems will increase the volume, complexity and variety of voice and non-voice emergency data.<sup>42</sup> These emergency calls include “voice, text, or video and related data.”<sup>43</sup> These calls also include “nonhuman-initiated automatic event alerts, such as alarms, telematics, or sensor data, which may also include real-time voice, text, or video communications.”<sup>44</sup> Each call includes location and other data, such as telephone number, personal information and accident information of VEDS.<sup>45</sup> Moreover, additional data from the call and external sources include personal and medical information.<sup>46</sup> These call and additional data can be analyzed through quantitative statistical methods and other analytics<sup>47</sup> to create usable call information to deliver to first responders, such as medical information to emergency medical technicians.

More emergency call data are usable information when they can be used by PSAPs and first responders to more effectively and efficiently provide emergency services, efficiently manage first responder agencies and coordinate emergency management and first responder operations. This information is most effective when it can be used to reduce notification times, reduce operational risks, identify incident threat levels, improve agency performance and improve allocation of resources.<sup>48</sup> Consider the example of how a NG911 call, public safety and private data can be useful to identify traffic, criminal and other incidents leading to a serious threat:

Let’s imagine two men rent a white van with cash and provide an international passport as proof of identification. Shortly there-after

---

<sup>41</sup> *Id.* at 6, 11, 13, 19–21.

<sup>42</sup> FCC, LEGAL AND REGULATORY FRAMEWORK, *supra* note 4, at 3.

<sup>43</sup> 47 U.S.C. § 942(e)(4)(A) (Supp. 2013).

<sup>44</sup> *Id.* § 942(e)(4)(B).

<sup>45</sup> NENA, ADDITIONAL DATA, *supra* note 2, at 6.

<sup>46</sup> *Id.* at 6, 19.

<sup>47</sup> See P'SHIP & IBM CTR., *supra* note 18, at 7 (stating that “[s]taff with good analytics know-how is critical for helping agency employees navigate the data”).

<sup>48</sup> See NAT'L 911 PROGRAM, *supra* note 17, at 3 (explaining that the National 911 Program finds that “[t]he value of the data comes from the story it tells . . . [and] [d]ata can be used to: [i]dentify problems, [r]efine problems, and [d]efine the questions that lead to solutions”).

a 3-1-1 center takes a call about a large white van blocking a road near a garden center. The vehicle is not there when officers arrive. Next, a white van was cited for having an inoperable tail-light while driving nearby on I-95 toward Washington DC. The next morning the garden center reports 12 bags of fertilizer missing.

Taken independently, each of these events is not significant, and may never be correlated. Were the incidents to happen in different jurisdictions it is highly unlikely that they would ever be put together, nevermind the fact that the rental data actually came [from] a private source. Now let's add in that across a 50 mile radius, over 100 bags of fertilizer had been reported missing. Suddenly the information taken in whole signifies a potential terrorist threat and the white van, for which we have license plates and driver descriptions and a route of direction becomes a prime suspect in a cross jurisdictional search.<sup>49</sup>

Many local incidents begin with 911 calls in a single jurisdiction, but a few calls may cover multiple jurisdictions and create the need to collect and correlate data across jurisdictions and disciplines (agencies).<sup>50</sup> Notwithstanding the benefits of more NG911 data and information, the collection and delivery of these data and information by telecommunication carriers, 911 service providers, PSAPs and first responder agencies raise legal, ethical, and public policy issues to provide emergency services.

### III. LEGAL & REGULATORY ISSUES REGARDING THE COLLECTION OF 911 CALL DATA

Legal and regulatory issues arise under federal communications law governing the collection, transfer and use of emergency call data for emergency services.<sup>51</sup> Federal communications policy governs the collection, delivery and use of emergency call data by telecommunications carriers and affects the collection and use of these data that are delivered by these

---

<sup>49</sup> Todd Piatt, *What is the Big Data Thing and Why Should the Public Care?*, RAVEMOBILESAFETY.COM (Mar. 21, 2013), <http://www.ravemobilesafety.com/big-data/>.

<sup>50</sup> See DEP'T OF HOMELAND SEC., NATIONAL INCIDENT MANAGEMENT SYSTEM 45 (2008), available at [http://www.fema.gov/pdf/emergency/nims/NIMS\\_core.pdf](http://www.fema.gov/pdf/emergency/nims/NIMS_core.pdf) (discussing how "incidents that begin with a single response discipline within a single jurisdiction may rapidly expand to multidiscipline, multijurisdictional incidents requiring significant additional resources and operational support").

<sup>51</sup> See FCC, LEGAL AND REGULATORY FRAMEWORK, *supra* note 4, at 3-4 (explaining the legal and regulatory issues arising under the federal communications law governing the collection, transfer and use of emergency call data for emergency services).

carriers to PSAPs and other emergency services agencies.<sup>52</sup> Any legal and regulatory issues that may arise in collecting, delivering and using emergency call data may involve privacy and use of personal data and predictive uses.

*A. Federal Communications Law Governing  
the Collection of 911 Data*

Federal communications statutes point to legal issues regarding the privacy of customer information and immunity from release of personal information to notify PSAPs and first responders.<sup>53</sup> This privacy regulation applies to telecommunications carriers by imposing “a duty to protect the confidentiality of proprietary information of, and relating to, other telecommunication carriers, equipment manufacturers, and customers.”<sup>54</sup> The carrier is prohibited from “using, disclosing, or permitting access to customer proprietary information obtained from its customers, either directly or indirectly through its agents.”<sup>55</sup> In the context of NG911 services, the carrier or its agents are granted exceptions to deliver customer information for emergency services.<sup>56</sup> One exception permits a carrier “to provide call location information concerning the user of a commercial mobile service . . . or the user of an IP-enabled voice service.”<sup>57</sup> Specifically, carriers can disclose call location information “to a public safety answering point, emergency medical service provider or emergency dispatch provider, public safety, fire service, or law enforcement official, or hospital emergency or trauma care facility, in order to respond to the user’s call for emergency services.”<sup>58</sup> The carrier can also disclose call location information “to providers of information or database management services solely for purposes of assisting in the delivery of emergency services in response to an emergency.”<sup>59</sup> Federal customer privacy regulation permits these carriers to disclose customer and call location information to PSAPs and

---

<sup>52</sup> *Id.* at 4.

<sup>53</sup> *See* 47 U.S.C § 222(a) (2012) (“Every telecommunications carrier has a duty to protect the confidentiality of proprietary information.”).

<sup>54</sup> *Id.*

<sup>55</sup> *Id.* § 222(d).

<sup>56</sup> *Id.* § 222(d)(4)(A).

<sup>57</sup> *Id.* § 222(d)(4).

<sup>58</sup> *Id.* § 222(d)(4)(A).

<sup>59</sup> *Id.* § 222(d)(4)(C).

other first responder agencies to provide emergency services.<sup>60</sup>

Federal privacy regulation must limit or restrict the disclosure and use of customer information but permit the use of emergency call data and predictive uses to provide more effective and efficient emergency services. This privacy regulation that prohibits the disclosure of call location information does not mean that customers permit carriers to use the call location and other information for commercial purposes, though these purposes may prove beneficial to providing emergency services.<sup>61</sup> Explicitly, federal privacy regulation states that “without the express prior authorization of the customer, a customer shall not be considered to have approved the use or disclosure of or access to<sup>62</sup> . . . call location information concerning the user of a commercial mobile service . . . or the user of an IP-enabled voice service.”<sup>63</sup> Moreover, this limitation on the use of call location information extends to “automatic crash notification information to any person other than for use in the operation of an automatic crash notification system.”<sup>64</sup> Thus carriers and 911 service providers that have access to call location and customer information cannot use this information for business purposes or disclose to the public, except for delivery of emergency services.<sup>65</sup>

*B. Impact of Cost on Collection & Delivery  
of 911 Data to PSAPs*

Customer privacy obligations and restrictions on disclosure and use of customer information do not allow carriers to use cost, an economic factor, to withhold data and information from PSAPs, first responder agencies or 911 service providers.<sup>66</sup> A carrier must provide call location and other information “on a timely and unbundled basis, under nondiscriminatory and reasonable rates, terms, and conditions to providers of emergency services, and providers of emergency support services, solely for

---

<sup>60</sup> *Id.* § 222(d)(4)(A).

<sup>61</sup> *See id.* § 222(f)(1) (stating that customer authorization is required prior to disclosure of “call information concerning the user of a commercial mobile service . . . or the user of an IP-enabled voice service”).

<sup>62</sup> *Id.*

<sup>63</sup> *Id.*

<sup>64</sup> *Id.* § 222(f)(2).

<sup>65</sup> *Id.* § 222(a), (d)(4), (f)(1)–(2).

<sup>66</sup> *See id.* § 222(g) (explaining that data must be provided to emergency service providers “under nondiscriminatory and reasonable rates, terms, and conditions”).

purposes of delivering or assisting in the delivery of emergency services.”<sup>67</sup> This cost obligation does not allow a carrier to impose unreasonable costs on the delivery of call location and customer information to PSAPs and first responders to provide emergency services.<sup>68</sup> However, the cost obligation does permit a carrier to use cost as means to deny the delivery to PSAPs and first responders of call location and customer information accompanying emergency call data that describe the emergency situation or event.<sup>69</sup>

Federal communications or 911 statutes address the liability and other protection for the release of subscriber call information by emergency communications providers and use of these data by PSAPs, persons and first responders. This 911 legislation establishes parity of protection among entities providing emergency communications and among users of 911 communications.<sup>70</sup> This legislation grants the “wireless carrier, IP-enabled voice service provider, or other emergency communications provider . . . [the same] . . . immunity or other protection from liability.”<sup>71</sup> that is granted to any local exchange company.<sup>72</sup> This immunity or protection is granted to service providers:

[I]n connection with an act or omission involving the release to a PSAP, emergency medical service provider or emergency dispatch provider, public safety, fire service or law enforcement official, or hospital emergency or trauma care facility of subscriber information related to emergency calls, emergency services, or other emergency communications services.<sup>73</sup>

Next, “[a] person using wireless 9–1–1 service, or making 9–1–1 communications via IP-enabled voice service or other emergency communications service[s]” are given the same “scope and extent of immunity or other protection . . . [as] a person using 9–1–1 service that is not via wireless 9–1–1 service, IP-enabled voice service, or other emergency communications service.”<sup>74</sup> Finally, PSAPs are given immunity and protection “[i]n matters related

---

<sup>67</sup> *Id.*

<sup>68</sup> *Id.*

<sup>69</sup> *Id.*

<sup>70</sup> See 47 U.S.C. § 615a(a)–(c) (2012) (stating that the “[p]rovider”, “[u]ser”, and “PSAP” are all granted immunity from liability).

<sup>71</sup> *Id.* § 615a(a).

<sup>72</sup> *Id.*

<sup>73</sup> *Id.*

<sup>74</sup> *Id.* § 615a(b).

**2015] BIG DATA & PREDICTIVE ANALYTICS 561**

to 9–1–1 communications via wireless 9–1–1 service, IP-enabled voice service, or other emergency communications service.”<sup>75</sup> Next, “a PSAP and its employees, vendors, agents, and authorizing government entity” are given the same scope and extent of immunity or other protection as a “PSAP, employees, vendors, agents, and authorizing government entity, respectively, in matters related to 9–1–1 communications that are not via wireless 9–1–1 service, IP-enabled voice service, or other emergency communications service.”<sup>76</sup> Although emergency communications providers, users and PSAPs are given immunity and other protection, they are limited to the same scope and extent of other parties and entities using or providing emergency call information.<sup>77</sup>

*C. Legal Issues Regarding Use & Privacy  
of 911 Data*

Although 911 and E911 services provide call location data, these services are limited by voice calls that cannot provide additional data.<sup>78</sup> The voice call describes the emergency situation but provides little call data, other than location data, in this situation.<sup>79</sup> The 911 and E911 communications systems do not ordinarily permit the delivery of non-voice data, text messages, videos and photographs or receive calls from alarm systems and automatic sensors.<sup>80</sup> However, current privacy restrictions and immunity and other protections explicitly recognize that NG911 voice and non-voice calls that include data, text messages and other information will be made by IP-enabled voice services.<sup>81</sup>

The use of analytics to analyze emergency call and additional data and make predictive uses may raise legal and regulatory

---

<sup>75</sup> *Id.* § 615a(c).

<sup>76</sup> *Id.*

<sup>77</sup> *Id.* § 615a(a)–(c).

<sup>78</sup> *See Guide: 911 Wireless Services*, FCC.GOV, <http://www.fcc.gov/guides/wireless-911-services> (last updated Dec. 5, 2014) (discussing how the location provided to emergency service providers is “not always specific enough for rescue personnel to deliver assistance to the caller quickly”).

<sup>79</sup> *See Piatt, supra* note 49 (explaining that a wide variety of data is often available, but only the location is often readily available since the data is “not structured or categorized”).

<sup>80</sup> FCC, LEGAL AND REGULATORY FRAMEWORK, *supra* note 4, at 8–9.

<sup>81</sup> *See* 47 U.S.C. § 615a(b) (“A person using wireless 9–1–1 service, or making 9–1–1 communications via IP-enabled voice service or other emergency communications service, shall have immunity or other protection.”).

issues. Predictive uses may not be information collected or provided by local exchange carriers, users and PSAPs.<sup>82</sup> For example, neighborhood and other social data that were collected from emergency situations and delivery of emergency services could be used to define the characteristics of a neighborhood.<sup>83</sup> These uses may aid first responders to respond to emergency calls by providing emergency services and assistance.<sup>84</sup> However, predictive analytics or uses that identify questionable personal behavior and associate it with customers who request emergency assistance may raise privacy issues regarding the disclosure of personal information. These predictive uses that were created from emergency call data to provide information may not be covered by privacy and immunity statutes. This lack of immunity protection and disclosure obligations may limit the use of predictive uses.

#### IV. ETHICAL QUESTIONS REGARDING THE COLLECTION OF 911 CALL DATA

Ethical questions may be raised by the collection and use of personal and other sensitive data by PSAPs and first responders. The disclosure of sensitive data may cause personal harm when predictive uses are not covered by privacy statutes and not subject to legal liability. Emergency call data that is subject to analytics that predict or show individual characteristics and activities may create ethical dilemmas, such as the disclosure of medical information.<sup>85</sup> Predictive uses that are made from emergency calls, medical or other data can cause PSAPs, first responders, and other persons to face ethical dilemmas.

##### A. *Personal & Other Sensitive Data Delivered to PSAPs*

NG911 services permit commercial organizations and 911 service providers to collect and deliver information to PSAPs and first responders that use this information to provide emergencies

---

<sup>82</sup> NENA, ADDITIONAL DATA, *supra* note 2, at 6.

<sup>83</sup> See, e.g., Piatt, *supra* note 49 (discussing how “sophisticated algorithms” are used to draw correlations between seemingly unrelated factors or events).

<sup>84</sup> *Id.*

<sup>85</sup> Crawford & Schultz, *supra* note 3, at 96–97 (“Alongside its great promise, Big Data presents serious privacy problems. Not only are the generated data sets sizable, but they also often contain very intimate aspects of individuals’ lives.”).

services.<sup>86</sup> This information is “associated with a call, a location, a caller and a PSAP,”<sup>87</sup> but comes from external “data sources.”<sup>88</sup> These organizations and providers also apply analytics to examine the data for tendencies, threats and trends and provide information and findings to PSAPs and first responders.<sup>89</sup> For example, a national 911 service provider uses big data and predictive uses to allow first “[r]esponders and PSAP personnel gain intelligent insight from billions of publically available commercial records about people, places and properties in an easy to read and interactive web-based format complete with risk index, headlines and ‘Be Aware’ statements.”<sup>90</sup> This provider gives PSAPs access to 120 million households.<sup>91</sup> Other information and predictive uses are taken from the following data:

Displays [of] relevant information on a street address or person of interest[;] Situational awareness and risk information, including vehicle ownership, criminal records, warrants, permits, property records, relatives, associates and Internet or social media posts[;] [and] Key contact data for address occupants, such as mobile phone numbers[.]<sup>92</sup>

In fact, customer proprietary network and location information that are part of emergency call information cannot be publicly disclosed by carriers and their agents<sup>93</sup> but family, criminal, property and social media data may be readily available and can be disclosed to PSAPs and first responders.<sup>94</sup> Medical and other personal information that is available through social media or personal websites may not be protected by privacy statutes and could be released or disclosed to the public.<sup>95</sup> These records

---

<sup>86</sup> 47 U.S.C. § 222(d)(4)(A) (2012).

<sup>87</sup> NENA, ADDITIONAL DATA, *supra* note 2, at 6.

<sup>88</sup> *Id.*

<sup>89</sup> *See, e.g., Beware*, INTRADO.COM (2014), <http://www.intrado.com/sites/default/files/solutions/beware/Beware.pdf> (discussing the company Intrado and its use of analytics to assist PSAP personnel and responders).

<sup>90</sup> *Id.*

<sup>91</sup> *Id.*

<sup>92</sup> *Id.*

<sup>93</sup> 47 U.S.C. § 222(c), (f) (2012).

<sup>94</sup> *See* INTRADO, *The What and Why of IP Capability*, in 3 NEXT-GENERATION 9-1-1: THE ESSENTIAL GUIDE TO GETTING STARTED 1, 4 (2014), *available at* <http://www.intrado.com/nextgen-9-1-1-guide> [hereinafter INTRADO, NEXT-GENERATION 9-1-1] (discussing the different kinds of information that are accessible through data in multiple formats).

<sup>95</sup> *See* Crawford & Schultz, *supra* note 3, at 96–97 (discussing the availability of personal and medical information through websites such as the social media

contain information that could be humiliating and embarrassing to persons needing emergency assistance. One must consider the moral obligations of 911 service providers to collect and disclose private information and PSAPs and first responders to use this information to provide emergency services.

*B. Use of Personal Data & Predictive Uses  
by PSAPs & First Responders*

Ethical questions are raised by the delivery to PSAPs of personal, behavioral, social and other information by 911 service providers and commercial organizations. This particular information is not prohibited by regulation and is not a part of the 911 emergency call data.<sup>96</sup> Personal information may include sex, ethnicity, behavioral traits, and family information that could be used by PSAPs to assist first responders responding to a particular emergency.<sup>97</sup> For example, family information could identify relatives and siblings that may need to be contacted in an emergency to assist in providing medical services to the victim. First responders who are informed of family information must decide how to use this information to avoid ethical dilemmas in seeking assistance of a family member. First responders who are provided personal information acquired from a social media website must decide whether to use this information to provide emergency medical, rescue and other services.<sup>98</sup> NG911 systems permit the delivery of more personal information that is acquired from external sources, reduces threats to first responders and improves emergency services to the public.<sup>99</sup>

---

site Facebook); *see also Beware, supra* note 89 (stating that social media and internet can be searched for information to assist first responders).

<sup>96</sup> *See* 47 U.S.C. § 222. The statute discusses the confidentiality and privacy requirements of carrier and customer information that is received. However, it does not include protection or regulations regarding personal information (proprietary or non-proprietary) that is received through outside channels, such as social media, or public information.

<sup>97</sup> *See generally* Crawford & Schultz, *supra* note 3, at 93–95 (discussing how different kinds of information can be discovered and used in first responder situations).

<sup>98</sup> *See* INTRADO, NEXT-GENERATION 9-1-1, *supra* note 94, at 4 (stating that mapping the most effective way to use data is an important feature when obtaining data).

<sup>99</sup> *See* INTRADO, *The What and Why of Next-Generation 9-1-1*, in 1 NEXT-GENERATION 9-1-1: THE ESSENTIAL GUIDE TO GETTING STARTED 1, 1–3 (2013), available at <http://www.intrado.com/nextgen-9-1-1-guide> (discussing the

*C. Ethical & Moral Harm of Disclosing 911 Data*

If the disclosure of predictive behavior and other uses delay or restrict emergency services and causes an individual or neighborhood to suffer more deaths, injuries or property losses, this disclosure creates an ethical dilemma for PSAPs and first responders. In addition, ethical questions may be raised by lapses or failures to collect and use data and predictive uses. For example, the failure to collect and deliver to PSAPs accurate location or other data, though lawful, could harm the public if these data could have been more accurate.<sup>100</sup> Ethical issues would be raised by the use of location data that could delay or hinder the dispatch of first responders when carriers comply with FCC regulations that require less than full implementation of location accuracy in some cases.<sup>101</sup> Carriers must decide whether or not to provide the most accurate information or allow the public to face delays in the delivery of emergency services caused by less than accurate information. Another example is the ethical dilemmas faced by PSAPs and first responders who must decide whether or not to use family background and other information acquired from commercial sources to provide emergency services. Although this information may be reliable and necessary, it was not received with the emergency call, and the emergency caller may not know of or contemplate the use of this information.<sup>102</sup> First responders and PSAPs must decide whether or not to use family or other personal information, though the victim or public

---

advantages of Next Generation 9-1-1 services in improving accuracy, safety, and transmitting information).

<sup>100</sup> See 47 C.F.R. § 20.18(h) (2015) (explaining that there are “location accuracy” standards that licensed PSAPs must comply with).

<sup>101</sup> FCC regulations do not require 100 percent accuracy for handset or network technologies and carriers, which exclude some areas of PSAPs and counties. The regulations provide: “(2) Handset-based technologies: (i) Two years from January 18, 2011, 50 meters for 67 percent of calls, and 150 meters for 80 percent of calls, on a per-county or per-PSAP basis. However, a carrier may exclude up to 15 percent of counties or PSAP service areas from the 150 meter requirement based upon heavy forestation that limits handset-based technology accuracy in those counties or PSAP service areas. (ii) Eight years from January 18, 2011, 50 meters for 67 percent of calls, and 150 meters for 90 percent of calls, on a per-county or per-PSAP basis. However, a carrier may exclude up to 15 percent of counties or PSAP service areas from the 150 meter requirement based upon heavy forestation that limits handset-based technology accuracy in those counties or PSAP service areas.” *Id.* § 20.18(h)(2).

<sup>102</sup> See Crawford & Schultz, *supra* note 3, at 94–95 (discussing a well-publicized news article about the department store Target collecting a customer’s information without her consent and utilizing it for sales purposes).

never contemplates the use and disclosure of this information.<sup>103</sup>

## V. PUBLIC POLICY CONCERNS REGARDING THE COLLECTION & DELIVERY OF DATA

Communications, privacy and other statutes may not address privacy, liability, disclosure and other concerns that limit the collection and use of big data and predictive uses. Foremost, these concerns must be addressed by legislative and regulatory policy-makers to permit big data and predictive analytics to improve delivery of emergency services. Moreover, big data and predictive analytics can improve policy-making in making legislative and regulatory decisions regarding the implementation and management of NG911 services and IP-based communications networks.<sup>104</sup>

### A. *Privacy, Liability & Other Public Policy Concerns*

The public policy concern is whether current 911 and communications legislation covers the use of additional data and predictive uses to provide emergency services that were once delivered by a voice only emergency call.<sup>105</sup> Carriers are not permitted to disclose customer proprietary network information that “relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier.”<sup>106</sup> Proprietary network information “is made available to the carrier by the customer solely by virtue of the carrier-customer relationship.”<sup>107</sup> The carrier is permitted to disclose “information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer

---

<sup>103</sup> See *id.* (explaining that the Target customer did not want her personal information revealed and Target did so without her permission).

<sup>104</sup> NAT'L 911 PROGRAM, *supra* note 17, at 3 (“Public policy makers are more likely to establish effective ‘decision systems’ if they are supported by ‘data systems.’ If agencies want to improve program effectiveness and efficiency, they need to manage performance, and to do so, they have to measure it.”).

<sup>105</sup> See NENA, NEXT GENERATION 9-1-1 TRANSITION POLICY IMPLEMENTATION HANDBOOK 23–25 (2011) [hereinafter NENA, IMPLEMENTATION HANDBOOK], available at [http://c.yimcdn.com/sites/www.nena.org/resource/resmgr/ngpp/ng\\_911\\_transition\\_policy\\_hand.pdf](http://c.yimcdn.com/sites/www.nena.org/resource/resmgr/ngpp/ng_911_transition_policy_hand.pdf) (discussing the shortcomings of traditional 911 data collection and legislative steps necessary to implement NG911).

<sup>106</sup> 47 U.S.C. § 222(h)(1)(A) (2012).

<sup>107</sup> *Id.*

of a carrier.”<sup>108</sup> As stated above, customer privacy statute grants an exception for the disclosure of customer information to PSAPs and other first responders.<sup>109</sup> As carriers collect more data and use more analytics to integrate and analyze these data, other information that is not customer proprietary network information can be acquired from other sources.<sup>110</sup> Although the customer privacy statute permits the disclosure of customer proprietary network information to PSAPs and first responders to provide emergency services, it is not certain that this disclosure includes the use of customer proprietary network information and predictive analytics to collect other data and information to improve delivery of emergency services.<sup>111</sup> Telecommunication carriers are entering big data and predictive analytics markets to provide emergency and other services to a number of industries.<sup>112</sup>

Telecommunications carriers and other service providers must ask if 911 legislation that grants immunity and other protection covers an “act or omission involving the release” to PSAPs and other first responders of big data and predictive uses that are not “subscriber information related to emergency calls, emergency services, or other emergency communications services.”<sup>113</sup> As stated in Part IV.A above, communications or 911 service providers have already begun to use big data and predictive analytics to provide more information to PSAPs and first responders and willing accept the legal risk and uncertainty of providing additional data.<sup>114</sup> More data include “relevant information on a street address or person of interest[,] . . . associates and [i]nternet or social media posts[,]

---

<sup>108</sup> *Id.* § 222(h)(1)(B).

<sup>109</sup> *Id.* at § 222(d)(4)(A).

<sup>110</sup> See *supra* note 95 and accompanying text (discussing the wide array of information that is available from social media and other sources).

<sup>111</sup> See MIND COMMERCE PUBL’G, BIG DATA AND TELECOM ANALYTICS MARKET: BUSINESS CASE, MARKET ANALYSIS & FORECASTS 2014-2019, at 8 (Sept. 2013), available at [http://www.mindcommerce.com/big\\_data\\_and\\_telecom\\_analytics\\_market\\_business\\_case\\_market\\_analysis\\_forecasts\\_2014\\_2019.php](http://www.mindcommerce.com/big_data_and_telecom_analytics_market_business_case_market_analysis_forecasts_2014_2019.php) (“With access to vast amounts of data sets, telecommunications companies are emerging as major proponents of the Big Data movement. Big Data technologies, and in particular their analytics abilities, offer a multitude of benefits to telecom companies including improved subscriber experience, building and maintaining smarter networks, reducing churn, and generation of new revenue streams.”).

<sup>112</sup> *Id.*

<sup>113</sup> 47 U.S.C. § 615a(a) (2012).

<sup>114</sup> See discussion *supra* Part IV.A.

[and] [k]ey contact data for address occupants.”<sup>115</sup>

*B. Limiting Liability of Telecommunications Carriers & Other Providers*

Although current communications statutes provide immunity to telecommunications carriers and other parties who collect and use emergency information to transmit 911 calls,<sup>116</sup> this immunity may not extend to the disclosure of some additional data and predictive uses to provide emergency services. Simply, the NG911 emergency call provides for the use of additional data, but it is not clear that privacy and disclosure provisions ever considered the volume of an emergency call that could be supplemented with family background, occupancy information, criminal records, spatial and other data.<sup>117</sup> An emergency call cannot have an unlimited volume, and personal privacy and security may justify the need to place a limit on this volume.<sup>118</sup> This limitation on the volume of call data would permit additional data to protect privacy and security and limit liability under federal and state privacy statutes.<sup>119</sup> In a business environment and litigious society, telecommunications carriers and other 911 service providers may be reluctant to expand the collection and delivery of emergency call and additional data and predictive uses. This reluctance is caused by the risk and uncertainty of delivering and disclosing these data. Moreover, PSAPs and first responders may need to consider privacy and disclosure concerns when they are using emergency call and additional information from external sources that may not have been permitted under federal and state privacy statutes.<sup>120</sup> The potential for privacy and disclosure concerns increases with the collection or use of big data and predictive analytics when uncertainty exists regarding the lack of immunity and exceptions

---

<sup>115</sup> *Beware, supra* note 89.

<sup>116</sup> 47 U.S.C. § 615a(a).

<sup>117</sup> *See* NENA, IMPLEMENTATION HANDBOOK, *supra* note 105, at 18 (discussing NG9-1-1 transition policy issues involving “[c]onfidentiality, disclosure and retention of 9-1-1 call and other emergency information”).

<sup>118</sup> *See id.* (stating that the objective is “[e]nsuring that information delivered over Next Generation 9-1-1 systems can be appropriately delivered to Public Safety Answering Points (PSAPs) and shared with emergency response organizations while conforming to applicable confidentiality, disclosure and information retention statutes and rules”).

<sup>119</sup> *Id.*

<sup>120</sup> *Id.* at 22–23.

for the delivery and disclosure of vital personal information to provide emergency services.

*C. Limiting Liability of PSAPs & First Responders as Users*

Federal 911 legislation grants PSAPs and first responders immunity and other protection for the use of 911 communications.<sup>121</sup> This immunity and other protection create parity of protection in providing 911 communications and emergency services to the scope and extent other communications service providers and first responders have been granted immunity and other protection.<sup>122</sup> When other parties and first responders have no immunity and other protection in dealing with 911 communications and emergency services, the PSAPs, first responders and communications service providers may lack immunity and other protection.<sup>123</sup> This uncertainty regarding immunity and other protection occurs when the volume and complexity of emergency call and additional data are quickly expanding.<sup>124</sup> Currently, an emergency service provider is offering to make delivery of additional information and prediction analysis to PSAPs and first responders to supplement and support PSAP and first responder operations.<sup>125</sup>

If current communications and 911 legislation do not limit the liability of PSAPs, first responders and 911 emergency service providers, the delivery and uses of some emergency call and additional data will raise state and federal policy concerns.<sup>126</sup> States would need to determine the volume of an emergency call and identify the kinds of additional data that could be delivered to and disclosed by PSAPs, and used by first responders.<sup>127</sup> PSAPs and first responders need to know that any emergency

---

<sup>121</sup> 47 U.S.C. § 615a(c).

<sup>122</sup> *Id.* § 615a.

<sup>123</sup> *Id.*

<sup>124</sup> See NENA, IMPLEMENTATION HANDBOOK, *supra* note 105, at 22.

<sup>125</sup> NENA, NG9-1-1 SYSTEM AND PSAP OPERATIONAL FEATURES, *supra* note 22, at 6–7.

<sup>126</sup> See F.C.C., LEGAL AND REGULATORY FRAMEWORK, *supra* note 4, at 11 (“Governance of legacy 911 is divided between the state and federal levels. At the state level, the structure and provision of 911 service by PSAPs is typically a state law matter, with some states further delegating aspects of 911 governance to the local level.”).

<sup>127</sup> See *id.* at 39 (recommending that “Congress should consider incentives for states to revise their liability regimes to provide appropriate protection for entities providing or supporting NG911 services”).

call information made available in an emergency call or by a request for additional information in a fluid emergency situation<sup>128</sup> would not expose them to tort, privacy or other liability if other parties were injured or harmed by the disclosure of this information. Legislative and regulatory policy-makers must recognize the risk of an emergency services mistake or unauthorized disclosure that may increase with the volume and complexity of emergency call and additional data. Most importantly, any severe limits on the use of emergency call and additional data and predictive threats and behaviors by PSAPs and first responders could inadvertently expose the public to increased risk of deaths, personal injuries and property losses.<sup>129</sup>

## VI. CONCLUSION

Big data and predictive analytics include emergency call and additional data. The greater volume and complexity of emergency call data are enlarged by more data within the call (videos, photographs and telematics) and expanded by multiple external sources (social media, building records and others). These data and uses can increase the effectiveness and efficiency of PSAPs and first responders to deliver emergency medical, law enforcement, fire and rescue and emergency management services. This effectiveness and efficiency may be restricted by social and legal risks and moral and legal uncertainties of collecting and delivering new kinds of emergency call and additional data for use by PSAPs and first responders.

The collection, delivery and use of emergency call and additional data raise legal issues, ethical dilemmas, and public policy concerns. The collection and use of emergency call and additional data and their predictive uses can improve the delivery of emergency services. Federal privacy and parity of protection statutes permit the delivery of emergency call information. It is uncertain whether these statutes contemplated the sheer volume and complexity of emergency call and additional data that can be delivered to PSAPs and first responders. These data include emergency call data (description and location), supplemental data (medical, spatial and situational), and supporting data (criminal, property, social media, and family). These data are also exposed to analytics and

---

<sup>128</sup> *Id.* at 39–40.

<sup>129</sup> *Id.* at 40.

**2015]            BIG DATA & PREDICTIVE ANALYTICS            571**

technology that include statistical and quantitative methods and analytical computer programs to forecast events and determine trends and tendencies. These issues, dilemmas and concerns are raised by the delivery and use of more emergency call and additional data and its analysis to allow PSAPs and first responders to improve emergencies services.