Received: 3 December 2017 | Revised: 27 February 2018 | Accepted: 28 March 2018 | Published on: 26 April 2018

DOI: 10.1002/spy2.23

SPECIAL ISSUE ARTICLE

WILEY

The Internet of Things and the Smart City: Legal challenges with digital forensics, privacy, and security

Michael M. Losavio[1] | **K. P. Chow**[2] | **Andras Koltay**[3] | **Joshua James**[4]

[1]Department of Criminal Justice, University of Louisville, Louisville, Kentucky,
[2]Department of Computer Science, University of Hong Kong, Hong Kong, China
[3]Department of Private Law, Pazmany Peter University, Budapest, Hungary
[4]School of Global Studies, Hallym University, Chuncheon, Republic of Korea

Correspondence
Michael M. Losavio, University of Louisville, Louisville, KY.
Email: michael.losavio@louisville.edu

The explosive growth of information and communications technologies (ICTs) as manifested in Smart Cities and the Internet of Things (IoT) creates more and more computable data with myriad benefits. They also produce ever more digital evidence of people's lives in all contexts, with commensurately greater potential risks to the safety and rights of citizens. Digital/computational forensics and analytics, used to combat crime, are the vanguard of the collision of these with public policy as to privacy and personal autonomy. They bring the evidentiary fruits of this technology directly to the policymaker, police investigator, and the judge. And to the marketer, stalker, and extortionist. We examine this technical-legal interaction and how it might inform as to privacy and security with the IoT and the Smart City.

KEYWORDS

computational, digital, forensics, law, policy, privacy, security

1 | INTRODUCTION

The Internet of Things (IoT) and the Smart City generate and collect unprecedented datasets on people. The IoT is a vast connection of more and more devices, particularly those in common consumer items and systems. It builds "… the pervasive presence around us of a variety of *things* or *objects*… which, through unique addressing schemes, are able to interact with each other and cooperate with their neighbors to reach common goals."[1] The Smart City is the interconnected and instrumented civic forum where data from public life is sensed, collected, and analyzed. The Smart City applies technology to urban problems, particularly information and communication technologies (ICT).[2] The Smart City and the IoT may share their data for richer data corpora and the associated analytical products. This pervasiveness of ICT makes possible unprecedented data profiles on the lives of citizens and the life of the city, all available to intelligent and exacting analytics as to what those citizens of the city do.

The Smart City uses both its own infrastructure network of sensors and data collection as well as those of private parties and the IOT. The IoT is more global and loosely structured, with sensors and networks of private individuals and organizations both private and governmental. They may share data at various levels, to be analyzed for various purposes. That includes use as evidence for forensic decisions, whether through voluntary or opportunistic data interactions in people's lives.

Both can optimize private and public services, whether for commerce, governance, convenience, or the provision of public and private goods. One of the most important is for public security and safety, primary functions in civil society. Public security protects the rights to life, to be free of personal and psychological injury, to possess physical things, to be free to think and to act and speak. It also protects the liberty to be left alone, to have a private sphere of personal autonomy. Legal digital investigation—whether public or private—in the age of the IoT invokes elements of information security, public security, and the legal regulation of public and private life. These may be in unprecedented ways not yet directly addressed by law or tradition.

Digital forensics addresses "… the uncovering and examination of evidence located on all things electronic with digital storage, including computers, cell phones, and networks."[3] Digital forensics and analytics—computational forensics—are used

for many types of decisions, such as employment, divorce, child custody, contract resolution, or criminal judgments. They require the provenance, integrity, and reliability of data be established. They discover things hidden yet revealed through data collection, storage, and analysis.

The data panopticon of the IoT and the Smart City may create threats to personal autonomy, personality, and privacy. Van Zoonen suggests a framework for empirical research as to privacy concerns relating to the Smart City that can "sensitize" city government to those concerns.[4] A related threat is data being used to harm someone physically or in other ways. Whether the threat arises from the state or a criminal, the risk of threats must be weighed with the good produced. Use of the data corpus created by the IoT and the Smart City for judicial and other types of decisions should comply with legal rules promoting just, reliable outcomes without abusing safety, rights, and liberties. This is especially true with transnational activities and where these rules, rights and liberties vary between nations.

Part of the risk with digital investigations is from evolving standards of the reliability of digital evidence, such as messaging origins from IP addresses or online digital photograph authentication.[5] Competence in digital investigations is a major concern. For example, in the United States a substitute seventh grade teacher faced 40 years in prison due, in part, to insufficient analysis of digital forensics evidence.[6,7] This damages the discipline's credibility and utility, and runs a risk of punishing the innocent. Lack of standards for practitioners and questions as to competence and ethical behavior within the discipline create their own problems.[8] These concerns apply to the use of data from the IoT and from the Smart City.[9]

This interplay is where the rules of law confront the facts of technology. Innovation in computing leads to new evidence, both as to form and scale, and tools for finding it. The law may adopt or may lag rapid innovation in the technology, making for uncertain outcomes. This is critical for IoT and Smart Cities as digital investigation moves from device forensics into analysis of multiple objects internetworked across multiple legal jurisdictions. This enlarges the technical, legal, and governance challenges.[10] The IoT and the Smart City bring a new scale and scope to e-evidence, from all types of governmental, commercial and consumer systems, into the "cloud" and beyond. Inadequate abstraction of objects as evidence, data complexity, diversity and heterogeneity, scale and validation, visualization and identity management challenge our grip on these growing data masses and how legal rules map to the technical implementation.[11,12]

These technical challenges are paralleled by legal ones struggling to assure reliable, competent, and just use. Legal scrutiny increases as standards for competence in digital forensics become known and applied, even as they change with the technology. Legal forensic concerns include error rates, invasions of privacy and "experts" who are not, yet there may be insufficient or poorly established foundations to decide if lawful and competent digital forensics evidence has been developed.

The technical-legal challenges of digital forensics mirror challenges for information security and assurance. Computational systems will become responsible for both the good and bad from their use in our lives. Threats to privacy and security come from not only the intrusion into private areas of people's lives but have also misinference as to those lives based on improper or incompetent analyses.

2 | GLOBAL CONCERNS

Electronic commerce, the IoT and more and more private data systems are global enterprises. Smart Cities manage global data exchange for transnational systems like air transport, movement of persons, and commercial logistics. With nation-states, each with its own laws and priorities for public security, and ICT infrastructure, coordination between countries and their laws is vital to avoid failure. The criminal case of *United States* versus *Ivanov* involved remote and unauthorized access to American servers from Russia.[13] And investigating U.S. officer used a US court order to authorize remote access to Russian server data that contributed to the imprisonment of Ivanov, without Ivanov's consent. In response, Russian state security filed criminal charges for illegal access without proper authority and outside the jurisdictional powers of the United States.[14]

The most significant initiative to systematically address these issues is the 52-nation treaty of the Council of Europe's *Convention on Cybercrime*.[15] It is a multination legislative solution balancing public security with the rights of people. The *Convention* is a framework for investigations and prosecutions of computer-related misconduct between members. It creates a common ground for technical definitions for informatics and computing.[16] It sets out substantive and procedural criminal laws adapted to ICT and transnational concerns.[17] With a common foundation of laws of the signatory nations, its principles and procedures aid international cooperation in the investigation and prevention of cybercrime.[18]

Signatory nations focus on harmonized criminal law regimes that provide protection from offenses against technical systems, data, and intellectual property.[19] The Convention' s *sui generis* protections relating to ICT systems and data provide for criminal law penalties in five categories:

1. access to a computer without or in excess of authorization,
2. interception of data without authorization,

3. interference with data without authorization,
4. interference with a system without authorization, and
5. misuse of devices.[20]

Nations harmonize their digital investigative procedures for the preservation, discovery and analysis of electronic evidence. These include expedited preservation of stored computer data and traffic data, disclosure and production of stored and subscriber data and search and seizure to assure data integrity and network access.[21]

The *Convention* also requires "adequate protection of human rights and liberties." These protections, reflecting similar concerns in many countries, address fundamental civil, political and human rights, and freedoms.

A number of technologically advanced countries, the Russian Federation and the Peoples' Republic of China, have not joined the *Convention*. But they may have equivalent bilateral cooperation agreements, such as Mutual Legal Assistance Treaties (MLATs) and Mutual Legal Assistance Agreements (MLAAs) with other countries.[22] These set out the terms of collaboration and legal actions and assist in the exchange of evidence and information in criminal and other matters. For example, although the People's Republic of China is not a signatory to the Convention on Cybercrime, it has a MLAA with the United States to assist with criminal matters.[23]

Other types of bilateral treaties may be used to promote transnational and international cooperation. The framework of the United States-India Cyber relationships sets out detailed cooperative, investigative, and security principles consistent with national law and international responsibilities.[24] Areas of cooperation range from coordinated cyber security best practices to real-time/near real-time data sharing on cyber threats. Collaborative research, development and implementation of ICT security infrastructure and law enforcement capabilities in cyber security and cybercrime investigation are addressed. This illustrates the greater level of protection needed with the growth of ICT in the IoT and the Smart City. The framework is a model for vital transnational cooperation as computer power and the risk of victimization grows.

3 | COMPARATIVE REVIEW OF LEGAL REGIMES OF DIGITAL FORENSICS AND INVESTIGATIONS AMONG NATIONS

Even with the Convention on Cybercrime, local laws reflect differing notions of the rights of states balanced against the rights of people, and the needs of public security balanced against the personal security of individuals. They also reflect different underlying structures of national law.

Anticipating the local laws for the technologies can help in their design through flexibility data control. This can aid downstream users avoid problems. By examining the legal regimes of several nations, common concerns and structures may be identified that can promote broader security and privacy rights while optimizing the benefits of the IoT and the Smart City.

3.1 | Hong Kong Special Administrative Region, People's Republic of China

The Hong Kong Special Administrative Region represents transition from British common law and statute to the laws of the People's Republic of China. Both are early adopters of ICT. Law enforcement and the academic community in Hong Kong have focused on cyber security and digital forensics. These efforts extend to the Smart City network for Hong Kong, its IoT and the myriad of personal data technologies.

The *Smart City Blueprint for Hong Kong Mobility* addresses transportation issues:

1. Intelligent transport systems and traffic management.
2. Public transport interchanges/bus stops and parking.
3. Environmental friendliness in transport.
4. Smart airport technologies.

These systems will include automatic road tolling, autonomous vehicle support, real-time parking information, real-time information to encourage bicycling/walking, and biometric and mobile check-in for seamless air transport.[25]

Other areas are "Smart Living" for a fully Wi-Fi connected city, digital payment, electronic ID, and support for the elderly, persons with disabilities, and healthcare. These will use fifth-generation mobile networks and big data analytics for real-time data transmission and sharing among government agencies and cyber security implementations. The Smart City implementations for Hong Kong will rely on the IoT.[26] This integration of personal devices and networked "things" will provide more data to drive its Smart City implementations.

Such systems offer tremendous benefits for public administration and citizen services. They are also high risk targets for disruption; cyber-attacks against Smart City/IOT transportation can exploit vulnerabilities and cause significant damage, ranging from privacy compromises to vehicle damage to the loss of life.[27,28]

Although there are extensive usages of big data analytics in the People's Republic of China by private data users as well as the government, there are hurdles use in Hong Kong. The Personal Data Privacy Ordinance has similar data principle principles as the European Union (EU).[29] It requires data holders comply with six data protection principles and gives data subjects rights of notice and control over their personal data. Those data principles regulate the purpose and manner of personal data collection, accuracy and retention requirements, use limitations, security mandates, transparency as to data users' practices and the right of the data subject to access information. Potential violations of privacy have been investigated by the Office of Privacy Commissioner for Personal Data, Hong Kong, on collection of excess data by data users. The General Data Protection Regulations (GDPRs) for EU citizen data regardless of location will impact big data analytics in Hong Kong through its interactions with EU nations. This may require further review to assure harmony between the EU GDPR and the Hong Kong Data Privacy Ordinance.

Hong Kong's early response to electronic malfeasance and evidence built a framework for continued protection of ICT in the IoT in the Smart city. The Interdepartmental Working Group of law enforcement agencies that produced the Computer Related Crime Report[30,31] This extended protections to computer and digital data. Computer forensics labs were established for forensic analysis and training, growing to cover networks, the Internet, and mobile phones.

Analysis and use of digital evidence is regulated under the Computer Crimes Ordinance (HK), and includes as property "any program or data held in a computer or in computer storage medium"[32] and "extending the meaning of criminal damage to property to misuse of a computer program or data." The Telecommunication Ordinance was extended to criminalize "obtains unauthorized access to any computer."

These amendments have expanded state authority for the investigation and prosecution of cybercrimes and digital evidence new technologies, especially that of the IoT as to personal attacks. It offers a framework for addressing potential attacks against the Hong Kong Smart City infrastructure and simplifies the requirements for evidence seizure, search, scope of investigation and prosecution needed to deter malfeasance and cybercrime and, where necessary, incapacitate the cyber criminals.

There has been discussion about use of these laws to prosecute violent civil disobedience activities via digital evidence. Many question whether such activists are really cyber criminals and if this is an appropriate use of these investigative and prosecution powers. The heightened surveillance powers presented by these technologies may create a trade-off with privacy.

3.2 | The Republic of Korea

The Republic of Korea is aggressively adopting IoT and Smart City concepts. Korea has growing number of companies making IoT devices for home and business purposes. Further, the city of Songdo has partnered with CISCO to develop one of the first Smart Cities. Songdo city uses data collection and analysis for almost all public services.[33]

At the government level, decision makers are interested in Smart Cities and their technologies. Companies such as LG and Samsung, however, are focusing more on the consumer market. LG's U+ Smart Home service has many Internet-connected devices, such as IP cameras, connected air purifiers, and air conditioners. U+ provides cloud services for these devices with a monthly fee. This service provides remote control for devices from a smart phone or web interface. The service automatically configures in-home devices to save energy. Samsung and smaller companies have similar services. Korean smart speakers similar to the Amazon Echo are popular, such as the NUGU from SK Telecom and the Kako Speaker. Both include a virtual assistant service and connect with popular Korean online services.

Although Korea has been aggressive in the development and consumption of IoT devices, there have been challenges. An IP security camera from a Korean service provider was sold as a way to monitor and communicate with your pets. The camera included a built-in speaker and could be remotely controlled. In 2017, customers started reporting the camera turning to watch them while the users were home (and not connected). Reports emerged that the cameras were being remotely controlled Chinese language audio coming through the security camera's speaker.

At the consumer level, in Korea and outside, IoT devices are being created to try to be the first in market. In our research we found software and hardware vulnerabilities in all new IoT devices, and in some cases, no practical attempt at security at all. As devices advance, security features are usually added, but currently IoT devices are similar to home access points in terms of security stance.

Legislators do not see Smart Homes or Smart Cities as different from technology that existed before. Korea has relatively strong hacking and data protection legislation, so special consideration has not been given to data generated from IoT devices.

Digital investigations of activity such as this are covered by the Criminal Procedure Act (CPA). A warrant is required for search and seizure. Warrants for digital evidence are written broadly as the exact devices may be unknown. CPA Articles

110-113 protect military, public and professional secrets from seizure. Consent from the "person in charge" is needed and may be denied based on "interests of the State."

South Korea collects large amounts of criminal justice data, including specific case data, through its criminal justice portal Korea Information System of Criminal-Justice Services (KICS). The KICS system and data are subject to data privacy laws. Law enforcement and external researchers have asked for more access to KICS data for research purposes. Projects on criminal data mining have been proposed, but legislation must be amended before such data analysis is allowed. This leaves the impact on privacy rights and personal autonomy equally unclear, including as to data generated by the IoT and in the Smart City.

Law enforcement, like legislators, are treating IoT devices similar to smart phone in investigations. South Korea has major smart phone manufacturers as well as digital investigation companies specialized in mobile device analysis. These companies have found new business in dealing with IoT devices. The underlying technologies of most modern devices are similar, so the same—or slightly adjusted—service offerings still apply. Law enforcement in South Korea is actively looking into IoT and smart device forensics and investigations. Prior strict data protection legislation, however, still applies. Nonetheless, integration of IoT data will assist law enforcement in its investigations.

3.3 | The Republic of Hungary

Similarly, Hungary's capital of Budapest is pursuing Smart City projects as a way to encourage citizens to take better actions for a better city.[34] Implementations include public transportation information application for facilitating transport.[35] Long-term urban planning for Budapest integrates Smart City technologies as a horizontal objective regarding government operations and development.[36] These include aspects of innovation, sustainable resources and economy, transportation, and open urban governance. Smart City initiatives have also expanded to smaller cities in Hungary, including Debrecen[37] and Szeged[38] (in collaboration with the Universities of Szeged and Pannonia). Huawei of China is one company that has begun to implement Smart City systems in Hungary.[39]

With such integration of ICT into municipal operations, security, and public safety for the systems will be vital. Public security and safety will build on the growing regime of Hungarian cybercrime law and procedures. Both the codification of cybercrime as a criminal offense and the spread of the use of electronic evidence and data in criminal proceedings in Hungary resulted from the Cybercrime Convention signed in 2001. This introduced new types of criminal offenses into the Hungarian Criminal Code (such as the codification of fraud committed by means of IT systems, breach of IT systems or data, crimes committed through the evasion of the technical measures aimed at protecting IT systems.[40] The signing of the Cybercrime Convention also signaled a new approach to the rules of data collection and handling in the course of criminal procedures (such as the obligation to retain the data stored in IT systems).[41]

Hungary does not have a Western European-style (such as the British) law enforcement system which, by delegating cyber intelligence to the competence of the local police authorities, uses qualified experts. Information technology and investigative and criminal procedures have not yet been integrated. The provisions of the Act on Criminal Procedure ("BET") allow the application of IT intelligence-gathering tools using both a traditional and special interpretation of the Act. Within the framework of these proceedings, just like medical examiners, IT experts can be engaged to supervise the appropriate storage of data in compliance with the BET. In addition to this, the detailed rules of evidence handling are set out in specific Hungarian decrees.

One of the shortcomings is that it does not include other systems under the umbrella of "traditional" searches of premises and so does not allow data stored on servers to be searched. There is no option of tracking the data generated in the course of usage of the Voice Over Internet Protocol (VOIP).

Secret data collection is part of cyber intelligence. Regulation began with the democratic political transition of 1989-1990 with significant changes to ensure compliance with the Constitutional Court. The Data Protection Act,[42] the BET and law enforcement legislation guarantee broad protection of personality rights in accord with the strict requirement of data collection being "tied to a specific purpose."

The Act on Electronic Communications has a key role in user identification as a service provider must retain the data collected for only a short period (for 1 year, or for certain sensitive data for half a year) and may not frustrate the technical implementation of the covert data collection. The Act guarantees direct access to user data passing through the service provider's system for those carrying out covert data collection, and does not account for protection of personal data or the right to protect privacy. This power of the investigating authority to request data from the communications service provider without approval of the public prosecutor raises serious concerns.

Since the democratic political transition and the codification of the Cybercrime Convention, there have clearly been efforts to rationalize the rules of cyber intelligence and to respect constitutional rights. The legal system is committed to ensuring increasingly strong protection of personality rights, although concerns remain as to privacy protection under this system.

3.4 | The European Union

Smart City implementation in the EU is supported by the European Innovation Partnership on Smart Cities in Communities of the European Commission, funded by the EU.[43] It focuses on city specific challenges across policy fields, from mobility to ICT, and works to integrate all stakeholders for solutions and governance. Scalable and transferable solutions are the goal of funded projects.

The laws of the nations of the EU focus on common issues for the protection of privacy and assurance of the reliability of evidence and outcomes. The EU in implementing major privacy protections in the face of the power of ICT and the growing data collections of the IoT and the Smart City. The GDPR of the EU will go into effect in May 2018, and will unify and enhance data protection for individuals within the EU.[44] It may also impact use of data generated by the IoT.

Though exemptions exist for some public security/law enforcement purposes, forensic use outside of these areas will be impacted. Furthermore, some rights may indirectly affect all areas, such as the right to data erasure. Data protection/data transfer regulations may constrain some forensic activities. Under Article 58, penalties for compliance failures with the GDPR are significant. For commercial entities finds may be as much as the greater of €10 million or 2% of global annual turnover if related to technical measures and, for certain key provisions, the greater of €20 million or 4% of global annual turnover.

Because the scope of the GDPR embraces all EU originating data, regardless of its ultimate location, it will have an impact on transnational data flows and data practices of countries outside of the EU. In this respect its privacy protections may be integrated into the technologies for the IoT and Of the Smart City to avoid any risk of noncompliance as well as assure access to European markets.

3.5 | The United States of America

Smart City initiatives are underway across the United States, with Los Angeles, New York, and Chicago leading the embrace of these technologies to upgrade services from streetlights to sanitation bins to autonomous vehicles.[45] Federal agencies are promoting its implementation; the US Department of Transportation, for example has issued its "Smart City Challenge" to develop ideas on Smart transportation systems.[46] the IoT continues to expand; the retail market for IOT is expected to expand from $3 billion in 2016 to $11 billion by 2025.[47] The US Department of Commerce has proposed for areas in which to advance the IoT: enabling infrastructure availability, crafting balanced policy and engaging users, promoting standards and technological advancement, and encouraging markets to implement IOT.[48] All of these Smart City and IOT initiatives must comply with an ad hoc privacy regime as the US does not have a comprehensive privacy regulatory regime like the EU.

The Fourth Amendment to the US Constitution prohibits *unreasonable* state searches. The Supreme Court rule is a government search or seizure is unreasonable and in violation of law when, without probable cause of a crime, it *violates a reasonable expectation of privacy*. Analysis of digital forensics issues in federal cases found that challenges for violating this were the most common attacks on the legality of the digital forensics use.[49] Such unreasonable state searches may lead to civil damages as well as criminal prosecution of the state actors involved.[50,51] This may be a particular risk for implementation of a Smart City system.

These legal protections are expanded by statutory privacy laws that further limit invasions of privacy. Together these restrict interceptions, access and use of data, metadata and addressing; these range from applications for a wiretap/interception to lesser showings to access stored data and collect metadata. American law includes money damages for invasions of privacy, with individual states creating broader criminal and civil liability for informational misconduct. It is a patchwork of privacy protections, in contrast to those of other countries. But they could apply to both Smart City activities and to IoT activities. In particular, the use and analysis of IOT data may in some cases lead to significant civil liability for the invasion of privacy as well as collateral injury from the use of that information.

There is wide disagreement among law enforcement, government, and commercial analysts as to what are legal concerns in digital forensics.[52] Law enforcement was far less concerned with "best practices" or data transmission privacy than government analysts. These and other differences limit effective governance within the discipline, leaving much to the courts to decide. And there is much less predictability for how regulation of Smart Cities and the data use from the IoT will evolve. This presents additional risks for those developing and implementing these technologies. We reference further aspects of the US legal regime below.

4 | LEGAL GUIDANCE PRESENT AND FUTURE

4.1 | Legal guidance and the lack of it in existing jurisprudence

Anticipating legal matters may aid the growth of the IoT and the Smart City. The implementation by the EU of the GDPR, a well-defined set of rules for the systems, in practice may produce unanticipated results One early indicator of things to come are judicial rulings and commentary on new conflicts that come before them well ahead of legislation.

Similar to the boundary examination in software testing, examination of jurisprudence at the novel extremes of electronic data-founded investigations can indicate the direction and limitations on such state investigations. Review of United States case decisions offer a qualitative analysis of current problems and possibilities for the future regulation. The reasoning and analyses therein can be and have been used by other jurisdictions in the interpretation of laws. The analyses may anticipate legislative and political controversies that will weigh the rights of citizens for privacy and autonomy against the needs of the state for public safety and security.

4.1.1 | Forensic data collection and analytics—how growing data sets threaten privacy

United States v. Jones was the first major US case to present issues of the impact of investigative data technology and analytics.[53] In *Jones* it was the use of GPS tracking devices feeding to a central system. That investigative power drew special comments from both liberal and conservative jurists. Justice Sotomayor, considered a liberal, felt inexpensive computer-mediated geospatial tracking could "*alter the relationship between citizen and government in a way that is inimical to democratic society*." (emphasis added) via GPS data monitoring, aggregation and analysis. It would give the police immense surveillance power that "…evades the ordinary checks that constrain abusive law enforcement practices." Justice Alito, considered a conservative, addressed the geospatial corpus: CCTV, automated tolling systems, automobile automatic notification systems, cellular telephones and other wireless devices, all data of the IoT and the Smart City. He suggested that while short-term monitoring would be reasonable, longer-term it would be an illegal invasion of privacy and was an area open to statutory privacy regulation. From either perspective, Smart City/IOT forensic data collection and analytics may be threats to privacy by their sheer power.

4.1.2 | Personal devices and their growing data threaten privacy

The massive growth in cellular telephone data capacity and diversity led the Supreme Court to put cell phone examination out of bounds without a court order or special circumstances: "modern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans 'the privacies of life." The Court in *Riley v California* extended protection to new forms of data collection and storage not granted smaller, more static physical media like notebooks precisely because of the new scale, and what it reveals.[54]

4.1.3 | Antiforensics versus information security—forcing decryption

One man's privacy app is another's sedition tool. Encryption is a foundation for the security of information and for efforts to avoid forensic analysis ("antiforensics"). Officials raise the question of whether technology, privacy and public safety are on a collision course due to encryption.[55,56]

The antiforensic/privacy protection conflict was the heart of the two federal cases pitting the US Department of Justice against Apple, Inc.[57,58] The United States in both cases sought to force Apple to circumvent the encryption of Apple iPhones. This went beyond warrant powers of the state to seize *existing* evidence, such as encryption keys or decryption systems, to force creation of a decryption tool that did not exist. This raised issues of due process/fairness and involuntary servitude under US law.

The first case in New York sought to have Apple crack a phone of a drug dealer, but that judge expressed doubt that Apple could be forced to do so. Then the United States government filed a second case to force decryption of an iPhone taken from one of the terrorists involved in mass killings in San Bernardino, California. This second legal action was a much more emotionally compelling case of a mass murder. That judge agreed with the government's position. But before either of these legal positions could be examined by higher-level courts, the Department of Justice retained a third-party to crack the encryption and thus brought an end to these legal actions without a clear resolution.

These cases showed split opinions on forced collaboration and digital forensics, but they did not resolve these issues. Encryption thwarts investigations on one hand while protecting disfavored opinion on the other. Its regulation and of those that make it are some of the most difficult issues to resolve, especially between nations with radically different views on private rights and public security.

4.1.4 | Transnational disclosure of digital evidence

Cloud services and distributed data networks may have global facilities across national boundaries. The United States Department of Justice sought customer emails stored on a Microsoft server outside of the United States. Microsoft refused and the court found no authority to authorize seizure of customer e-mails stored exclusively on foreign servers.[59] Despite this, the Department of Justice sought a similar order against Google from a different federal court. Despite support for Google from Microsoft, Amazon, Cisco Systems, and Apple, that court ordered Google produce information on servers located outside of the United States.[60]

This conflict in law is not yet resolved and maybe soon resolved by the US Supreme Court, but there is still only conflicting guidance on territorial limits to pursuit of electronic evidence.[61] This territorial conflict applies both ways, leaving open the rights of other countries to access data where they wish.

The legal guidance offered by these case decisions indicates both the efforts that will be made by states to exploit data systems for public security and possible responses to limit that exploitation as to protect the rights of peoples.

4.2 | Legal concerns for the future

As these cases show, weighing the needs of the state against the rights of citizens will be a central challenge for lawful implementations of the IoT/Smart Cities and the related digital forensics needed for public security. The evolving, massive growth of our data personae and powerful analytics require dynamic legal responses. Expectations of privacy are not limited to cell phones but may apply everywhere, to tablets, health, exercise and medical systems, automobile OBD/EVD systems and our tools of the IOT. This is such a rich source of evidence that conflicts between police power and the rights of citizens is assured; the scale of that conflict will depend on the laws of each nation. Yet this is also novel we may not he have even a clear sense of proper and ethical behavior in this area.[62]

From these general legal principles and the analyses in these cases, we can anticipate some of the areas for conflict. For the IoT this might be very disruptive as devices are broadly distributed to people such that interference with them is interference in their lives. It may similarly impact Smart City implementations where components, like transportation transponders or services chips, are held and used by the people in the city.

4.2.1 | The seizure of data and data containers

Traditionally law enforcement who had the right to seize the containers of evidence. It may lead to seizure of all such devices upon evidence of misconduct, no matter how disruptive. For example, required automobile event data recorder systems that record speed, acceleration and other factors might be seized for traffic offense.[63,64] While this may be onerous, it may be permissible absent a clear statement in law to the contrary.[65] Each IOT device that may carry information regarding an event becomes an evidentiary object. If the event engenders a criminal investigation, that device may be seized in order to secure the evidence, even without a court order. If the event relates to a civil action, then it may be subject to a court order to be produced and examined by an opposing party. This may both enhance the pursuit of truth as to an event at the cost of significant inconvenience to the device holder.[66]

4.2.2 | Encryption

The *Apple* litigation suggests a two-track security race in technology.[67] The first is development of better and stronger encryption. The second is "…to build a legal team to keep the government out of users' phones." This may be an arduous legal process to determine who is right. While many nations require technology companies create back-door access to their encryption, this would conflict with the laws of other countries and their protections for the right to speak anonymously, especially when criticizing government.

This may be such a fundamental issue for the US that only judicial resolution can settle the issue. Technology companies have no clear rules to guide them. Relations between nations on this may lead to conflict, ranging from privacy protections of the EU to those of nations that subordinate encryption to national laws. This may become an international conflict with wide and vastly expensive repercussions for commerce and government.

4.2.3 | Third-party data collection, storage and exchange, and the analytical data personae

The IoT and the Smart City will engender huge growth in third-party data collection and storage, which will only expand with the IoT, presents new challenges to privacy and personal autonomy. The EU has structured, well-developed regulations with rigorous controls on data collection, storage, transmission, and use. Other countries, including the United States, do not.

Traditional legal principles in the United States provide few restrictions on data either voluntarily given or collected by third parties, data that powerful analytics can you to divine even intimate facts. The Supreme Court will decide if police access to cellular telephone third-party data collections is restricted by the Constitution.[68] How other countries handle this may be guided by their customs of balancing citizen rights against those of the state or by were develop statutory regimes relating to these issues. Given the growth of global data exchange and the power of analytics, this is an area subject to both national legislative solution and international treaty cooperation.

4.2.4 | Transnational data distribution

Legislation and jurisprudence begin at home. The expansion of global data storage and analysis and of privacy protecting technologies set up a clash between states, nongovernmental organizations and the people that use the technologies. A successful seizure of data located in one country by officials in another may set up a conflict between nations or make impossible some transnational operations by technology companies. This, too, is an unresolved aspect of the legal regime of digital forensics.

It is an area particularly appropriate for treaty collaboration between nations on digital forensics and information security. Although the privacy protections of the GDPR of the EU are not matched in many countries, the EU asserts extraterritorial application to data originating on EU subjects. Given global trade, this may effectively extend the GDPR's compliance requirements internationally.

4.2.5 | Computational forensics, crime, and national security

AI forensics analysis, predictive policing and criminal justice decision-making via algorithmic analysis of data sets are growing. These technologies—effectively Big Data in the Smart City—are central to the Smart City and fully using the IoT.[69] They advise on prison sentences, pretrial release and parole decisions. The reliability of inferences may be used for investigative stops, "frisks," searches, arrests, and convictions. These raises concern as to precision, accuracy and reliability, especially with potential biases in the coding that go undetected.

Criminal justice use of forensic predictive algorithms must be vetted for illegal or unfair biases, sufficiency for individualized inferences regarding criminal activity and compliance with defined legal standards.[70] Reliability and fairness are vital; the use of bad data, biased algorithms and historical practices could introduce error in outcomes. This highlights risks with these technologies, especially in law enforcement, that may become laws in this domain.

Conversely, the growth of these systems as to raise concerns about the liberties of people also reveals targets and vulnerabilities. By collecting such rich data these systems become valuable targets for criminal cyber attacks. Security of the systems from such will become a priority, especially as liability law begins to encompass failures to protect and customers themselves insist on protection in exchange for consumer loyalty.

Similarly, the power and pervasiveness of the IOT and Smart City systems also make them potential vulnerabilities for national security. This has also been the subject of political discourse. The largest telecommunications equipment manufacturer in the world deploys its systems, from networking to smart phones, around the world. This includes major Smart City initiatives, as noted above. Yet the dominance of such key manufacturers creates concerns regarding national security as systems are deployed around the world.[71]

5 | CONCLUSION

Shari Pfleeger wrote "… with our great computing power comes great responsibility—to use our power wisely…" Digital forensics, a reflection of digital security and privacy, is especially sensitive to this. The resolution of legal application of digital forensics among and across nations will also guide these issues on the future of information security and assurance. How we balance the risks and benefits of massive data technology will define the relationship between the government and the governed in the information polity.

This is no mere question of "what do you have to hide?." Digital forensics is about finding things. But personal autonomy, the idea of personality that subsumes rights of privacy, gives the individual to right to keep control of certain things. Balance is needed, and that balance is best achieved through legislative rulemaking. Treaty agreement between nations can help the transnational conflicts that will inevitably arise. But the issues are broad.

Encryption, analytics, the IoT, "Big Data," Smart Cities and transnational data systems make this a complex mix of national sovereignty and politics. But it is essential to start the discussion.

And this discussion of balance, laws and treaties will support information security and assurance. It may be guided by the evolution of ethical codes for the discipline. While this goes beyond existing professional obligations in information security and assurance, it is a guide for the future of that greater domain.

Justice Sotomayor said in *Jones* these information technologies may damage the liberties we need to be the people we are. They impact every nation that values the rights of its people. It must be carefully balanced against the risks of criminal and terroristic actions threating peace and stability.

The consequences of this huge new data space for our privacy, security and rights of personality and personal autonomy may be significant. At this boundary between security and citizen rights, a judicial resolution might not be satisfactory, or even possible. This needs clear legislation of what can and cannot be done in balancing public security with individual freedoms.

We must address them, reflecting upon our traditions of freedoms weighed against the public security challenges of these new technologies, now and for the future. Failing may very well change who we are, and who we want to be.

ORCID

Michael M. Losavio http://orcid.org/0000-0003-4542-8599
K. P. Chow http://orcid.org/0000-0003-4552-9744
Joshua James http://orcid.org/0000-0003-0148-4732

REFERENCES

1. Giusto D, Iera A, Morabito G, Atzori L, eds. *The Internet of Things*. Heidelberg, Germany: Springer; 2010.
2. Dameri RP. Searching for smart city definition: a comprehensive proposal. *Int J Comput Technol*. 2013;11(5):2544-2551.
3. Garfinkel S. Digital forensics. *Am Sci*. 2013;101(5):370.
4. Van Zoonen L. Privacy concerns in Smart Cities. *Govern Inform Quart*. 2016;33:472-480.
5. Losavio M, Keeling D. Evidentiary power and propriety of digital identifiers and the impact on privacy rights in the United States. *J Digit Foren Secur Law*. 2014;9(2):197-203.
6. Krebs B. Substitute Teacher Faces Jail Time Over Spyware. *Washington Post*; 2014.
7. Eckelberry A, Dardick G, Folkerts J, et al. *Technical Review of the Trial Testimony: State of Connecticut vs. Julie Amero*; 2007. http://sunbeltblog.eckelberry.com/wp-content/ihs/alex/julieamerosummary.pdf. Accessed February 20, 2018.
8. Losavio M, Seigfried-Spellar KC, Sloan JJ III. Why digital forensics is not a profession and how it can become one. *Crim Justice Stud*. 2016;29(2):143–162.
9. Elmaghraby A, Losavio M. Cyber security challenges in Smart Cities: safety, security and privacy. *J Adv Res*. 2014;5(4):491-497.
10. Garfinkel S. *Digital forensics research: the next 10 years. Proceedings of the Digital Forensics Research Workshop 2010, Portland, Oregon*, 2010, Elsevier.
11. Lillis, D, Becker, B, O'Sullivan, T, Scanlon, M. "Current Challenges and Future Research Areas for Digital Forensic Investigation" (2016). Annual ADFSL Conference on Digital Forensics, Security and Law. 6. Accessed April 9, 2018 https://commons.erau.edu/adfsl/2016/tuesday/6
12. Raghavan KT. *Digital forensics: defining a research agenda.*, 2013 46th Hawaii International Conference on System Sciences (2013) Wailea, Maui, HI USA. IEEE Computer Society.
13. Conn D. *United States vs. Ivanov*, 175 F Supp. 2d 367; 2001.
14. Janke A. *A Hacker Story*. CIO Asia; 2005, Singapore.
15. Council of Europe CETS No. 185. *Convention on Cybercrime*, opened for signature; November 23, 2001. http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm. Accessed February 20, 2018.
16. Council of Europe Convention on Cybercrime, Chapter I, Article 1. ETS No. 185; November 23, 2001.
17. Council of Europe Convention on Cybercrime, Chapter II. ETS No. 185; November 23, 2001.
18. Council of Europe Convention on Cybercrime, Chapter III. ETS No. 185; November 23, 2001.
19. Council of Europe Convention on Cybercrime, Chapter III, Section 1, Articles 2–4. ETS No. 185; November 23, 2001.
20. Council of Europe Convention on Cybercrime, Chapter II, Section 1, Articles 2–6. ETS No. 185; November 23, 2001.
21. Council of Europe Convention on Cybercrime, Chapter II, Section 1, Articles 16–21. ETS No. 185; November 23, 2001.
22. Report on Treaties and Agreements. Bureau of International Narcotics and Law Enforcement Affairs, US Department of State, 2014 International Narcotics Control Strategy Report; 2014.
23. US-People's Republic of China Agreement on Mutual Assistance in Criminal Matters, Entered into Force; March 8, 2001.
24. Framework for the US-India Cyber Relationship. US Embassy in India. https://in.usembassy.gov/framework-u-s-india-cyber-relationship/. Accessed February 20, 2018.
25. Hong Kong Smart City Blueprint. *Innovation and Technology Bureau*. Government of the Hong Kong Special Administrative Region; 2017, Hong Kong SAR, China.
26. Hankinson M. *Honk Kong's Future as a Smart City Depends on the Internet of Things*. South China Morning Post; 2017, Hong Kong SAR, China.
27. Eden T. Car Hacking – With Bluetooth OBD; June 12, 2012. http://shkspr.mobi/blog/2012/12/car-hacking-with-bluetooth-obd/. Accessed February 20, 2018.
28. Yadav A, Bose G, Bhange R, Kapoor K, Iyenga NCSN, Caytiles RD. Security, vulnerability and protection of vehicular on-board diagnostics. *Int J Secur Appl*. 2016;10(4):405-422.
29. Personal Data Privacy Ordinance of Hong Kong. http://www.edb.gov.hk/attachment/en/sch-admin/admin/about-sch/personal-data-ordinace-cap486-note/privacy.pdf. Accessed April 9, 2018.
30. Report, Inter-departmental Working Group on Computer Related Crime, Hong Kong. https://www.infosec.gov.hk/english/ordinances/files/computerrelatedcrime&uscore;eng.pdf. Accessed July 5, 2017.
31. Crimes Ordinance, Ch. 200A – 221 I, Hong Kong. https://www.elegislation.gov.hk/. Accessed July 5, 2017.
32. Act C of 2012 on the Criminal Code; Articles 375, 423, 424.
33. Cities of the Future: Songdo, South Korea, Cisco Technology News. https://newsroom.cisco.com/songdo. Accessed February 27, 2018.
34. Criminal Procedure Act, Republic of Korea.
35. Smart City Budapest. http://smartcitybudapest.eu/. Accessed February 20, 2018.
36. Smart City Boot Up last Transport. http://en.smartcity.hu. Accessed February 20, 2018.
37. Smart Budapest Summary. *The Smart City Vision of Budapest*. Municipality of Budapest. http://budapest.hu/sites/english/Documents/Urban%20Development%20Plans/Smart&uscore;Budapest&uscore;summary&uscore;ENG.pdf. Accessed February 20, 2018.
38. Debrecen Smart City. http://smartcity.debrecen.hu/en. Accessed February 24, 2018.
39. Academic-Private Partnership for Hungarian smart city project, *Budapest Business Journal*; January 4, 2018.
40. Huawei Builds Smart City Nervous System. *Budapest Business Journal*; November 29, 2017.
41. Act XIX of 1998 on Criminal Procedure; Article 158/A.
42. Act CXII of 2011 on Informational Self-determination and Freedom of Information.
43. General Data Protection Regulation of the European Union.
44. European Innovation Partnership on Smart Cities and Communities. https://ec.europa.eu/info/eu-regional-and-urban-development/topics/cities/city-initiatives/smart-cities&uscore;en. Accessed February 20, 2018.

45. Liles S, Rogers M, Hoebich M. *A survey of the legal issues facing digital forensic experts*. In: Peterson, Shenoi, eds. *Chapter 20: Advances in Digital Forensics V*. Heidelberg, Germany: Springer; 2009:267-276.
46. Deans D. Exploring top smart city projects in the United States. *Telecoms Tech News*; September 11, 2017.
47. US Department of Transportation. Smart City Challenge. https://www.transportation.gov/smartcity. Accessed February 26, 2018.
48. Statista. Size of the Internet of Things in Retail Market in the United States from 2014 to 2025. https://www.statista.com/statistics/688756/iot-in-retail-market-in-the-us/. Accessed February 26, 2018.
49. US Department of Commerce. Green Paper: Fostering the Advancement of the Internet of Things; January 12, 2017.
50. Big Data: A Report on Algorithmic Systems, Opportunity and Civil Rights. Executive Office of the President (US); May, 2016. https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/2016&uscore;0504&uscore;data&uscore;discrimination.pdf. Accessed July 5, 2017.
51. 42 United States Code 1983 (US).
52. 18 United States Code 241, et seq. (US).
53. Cole KA, Gupta S, Gurugubelli D, Rogers M. "A Review of Recent Case Law Related to Digital Forensics: The Current Issues" (2015). Annual ADFSL Conference on Digital Forensics, Security and Law. 2. https://commons.erau.edu/adfsl/2015/wednesday/2 Accessed April 9, 2018
54. *United States v. Jones*, 132 S.Ct. 945 (2012) (US).
55. *Riley v. California,* 134 S.Ct. 2473 (2014) (US).
56. *Remarks of James Comey, Dir., Federal Bureau of Investigation. Going Dark: Our Technology, Privacy, and Public Safety on a Collision Course*. Washington, DC: The Brookings Institution; 2014.
57. Finklea K. Encryption and Evolving Technology: Implications for US Law Enforcement Investigations. Congressional Research Service Report 7-5700; February 18, 2016.
58. *In Re Order Requiring Apple Inc. to Assist in the Execution of a Search Warrant Issued by the Court, case number 1:15 – MC – 01902*. United States District Court for the Eastern District of New York.
59. *In the Matter of the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD20*. United States District Court for the Central District of California; 2016.
60. *In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation*. 829 F.3d 197 (2nd Cir. 2016 (US)).
61. In re Google Inc. N.D. Cal., No. 16-mc-08263, review denied 8/14/17.
62. *United States v. Microsoft Corporation*. Docket No. 17-2, Supreme Court of the United States on Petition from the Second Circuit Court of Appeals, *case pending*.
63. Losavio M, Seigfried-Spellar K, Sloan J. Why digital forensics is not a profession and how it can become one. *J Crim Justice Stud*. 2016;29(2):143–162.
64. 49 Code of Federal Regulations 563.7 (US).
65. Kerr O. The Fourth Amendment and Access to Automobile "black boxes." *The Volokh Conspiracy/Washington Post*; March 30, 2017.
66. Losavio M, Pastukov P, Polyakova S. Cyber black box/event data recorder: legal and ethical perspectives and challenges with digital forensics. *J Digit Forensics Secur Law*. 2016;10(4):43-57.
67. Baldwin R. The Apple Versus DO J Encryption Battle is Far from Over: The Legal Battles Between the Government and Tech Companies are Just Beginning. *Engadget*; March 29, 2016.
68. Simmons R. Quantifying Criminal Procedure: How to Unlock the Potential of Big Data in Our Criminal Justice System. 2016 Mich. St. L. Rev. 947; 2016.
69. *Carpenter v. United States*. Docket No. 16-402, Supreme Court of the United States, on Petition for Writ of Certiorari from the Sixth Circuit Court of Appeals, *case pending*.
70. Abaker I, Hashem T, Chang V, et al. The role of big data in Smart City. *Int J Inform Manag*. 2016;36(5):748-758.
71. Finley K, Newman L. Proposal for Federal Wireless Network Shows Fear of China. *Wired Magazine*; January 29, 2018.

How to cite this article: Losavio MM, Chow KP, Koltay A, James J. The Internet of Things and the Smart City: Legal challenges with digital forensics, privacy, and security. *Security and Privacy* 2018;1:e23. https://doi.org/10.1002/spy2.23