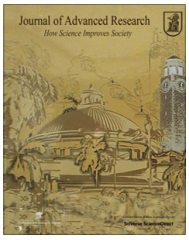
Journal of Advanced Research (2014) 5, 491–497

Cairo University

Journal of Advanced Research



ORIGINAL ARTICLE

Cyber security challenges in Smart Cities: Safety, security and privacy

Adel S. Elmaghraby *, **Michael M. Losavio**

Computer Engineering and Computer Science Department, 211 Duthie Center for Engineering, University of Louisville, Louisville, KY 40292, USA

ARTICLE INFO

Article history:
Received 29 October 2013
Received in revised form 4 February 2014
Accepted 25 February 2014
Available online 5 March 2014

Keywords:
Smart City
Internet of Things
Security
Privacy protecting systems
Security and privacy models

ABSTRACT

The world is experiencing an evolution of Smart Cities. These emerge from innovations in information technology that, while they create new economic and social opportunities, pose challenges to our security and expectations of privacy. Humans are already interconnected via smart phones and gadgets. Smart energy meters, security devices and smart appliances are being used in many cities. Homes, cars, public venues and other social systems are now on their path to the full connectivity known as the "Internet of Things." Standards are evolving for all of these potentially connected systems. They will lead to unprecedented improvements in the quality of life. To benefit from them, city infrastructures and services are changing with new interconnected systems for monitoring, control and automation. Intelligent transportation, public and private, will access a web of interconnected data from GPS location to weather and traffic updates. Integrated systems will aid public safety, emergency responders and in disaster recovery. We examine two important and entangled challenges: security and privacy. Security includes illegal access to information and attacks causing physical disruptions in service availability. As digital citizens are more and more instrumented with data available about their location and activities, privacy seems to disappear. Privacy protecting systems that gather data and trigger emergency response when needed are technological challenges that go hand-in-hand with the continuous security challenges. Their implementation is essential for a Smart City in which we would wish to live. We also present a model representing the interactions between person, servers and things. Those are the major element in the Smart City and their interactions are what we need to protect.

Introduction

The benefits of Information and Computing Technologies (ICT) in a Smart City and of the Internet of Things are tremendous. Smart energy meters, security devices, smart appliances for health and domestic life: these and more offer unprecedented conveniences and improved quality of life. City infrastructures and services are changing with new interconnected

* Corresponding author. Tel.: +1 502 852 0470; fax: +1 502 852 4713.
E-mail address: adel.elmaghraby@louisville.edu (A.S. Elmaghraby).

Peer review under responsibility of Cairo University.

2090-1232 © 2014 Production and hosting by Elsevier B.V. on behalf of Cairo University.
http://dx.doi.org/10.1016/j.jare.2014.02.006

systems for monitoring, control and automation. These may include water and sanitation to emergency responders and disaster recovery.

These benefits must be considered against the potential harm that may come from this massively interconnected world. Technical, administrative and financial factors must be weighted with the legal, political and social environment of the city.

Methodology

Several paradigms and categorical structures may be applied in analyzing the benefits and detriments of this data environment. An applicable paradigm used for this analysis is that of IBM that the Smart City, its components and its citizens are

- Instrumented
- Interconnected and
- Intelligent.

This is denoted as "IN3."

"Instrumented" gives city components and citizens devices, at varying levels of features that, at a minimum, respond to a sensor network. These are, in turn, "interconnected" as to pass information into a network. That information is computationally available for analysis and decision-making, making the Smart City "intelligent" in its operations.

Security and privacy concerns rest on how the information within IN3 is used. The core of the technology is the information. A full examination of any system of the Smart City may categorize information as to sources, types, collections, analytics and use (see Figs. 1–4).

The instrumented source may have particular rights or risks associated with particular types of information, such as a person's location or actions. The collections of that information, such as on the device or on a cloud aggregator, similarly invoke issues of rights, duties and risks. From those collections analytics can build services of varied sophistication which, in turn may be used for good or ill.

The loci of activity nodes may be categorized in relation to people, workplace, transportation, homes and social/commercial interactions.

An additional way to categorize within this space is to consider information source nodes as the activities and services of social and civic life, people, work, home, transport and social life.

In all of the interactions the information generation and exchange is at least bilateral and communicative. Actions often

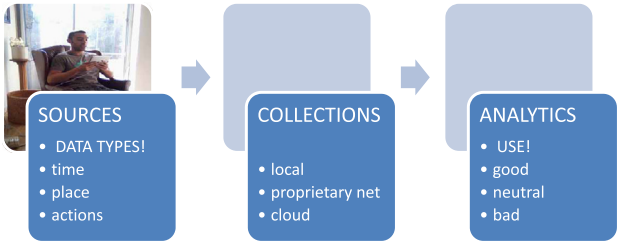


Fig. 1 Data sources feed data collections feed data analytics for knowledge.

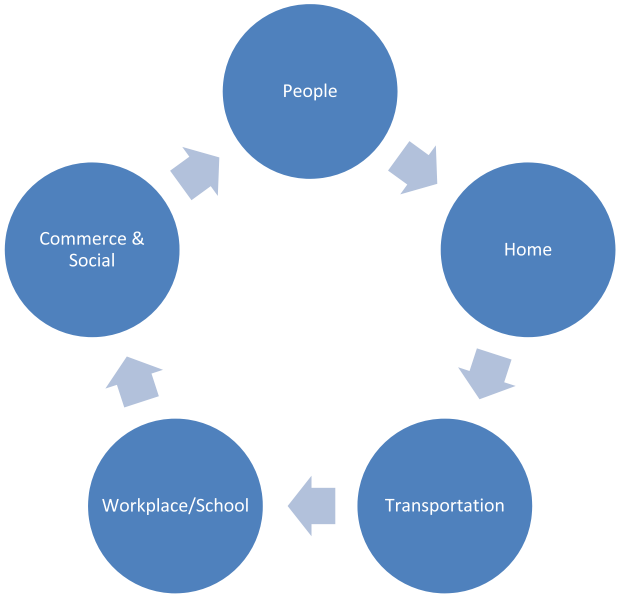


Fig. 2 The production loci of data in the Smart City.

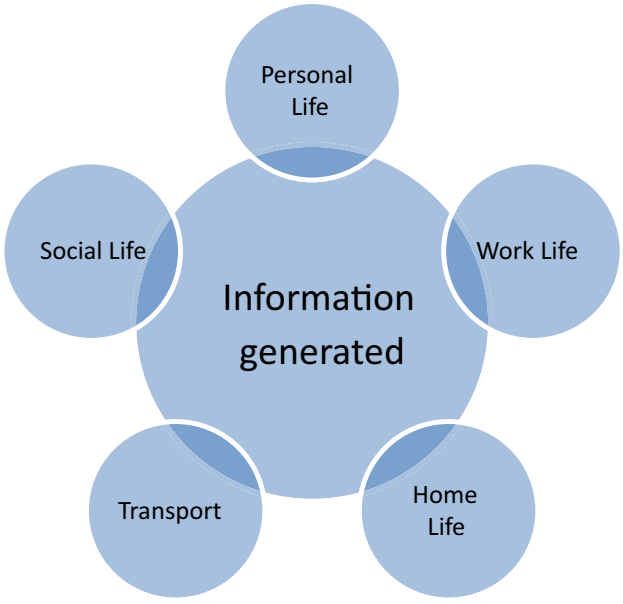


Fig. 3 Source nodes of activities and services producing data.

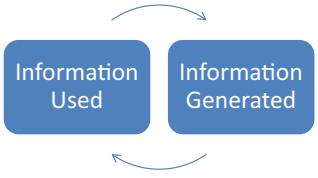


Fig. 4 The recursive cycle of data in the Smart City – information generated is information used is information generated is information used.

call and use information which, in turn, generates new information related to the services, including bettering those services on analysis.

IN3 is brought together in the commercial culture of search, recommender services and locational apps for devices that suggest services based on a person's location, characteristics and historical preferences.

More fundamental civil services at greater efficiency and reduced cost are possible for a Smart City. Citizen safety is a paramount civil responsibility. After the murder of a social worker making a home visit, computer engineering students devised an app package for smartphones that would track via GPS and provide panic button notification to supervisors and police via direct activation and timed cancelation. This support was only possible with this instrumented, interconnected and intelligent system. Similarly, every police officer on patrol may be monitored as to his or her precise location in relation to other activity in the city.

Yet this is subject to abuse. Various apps subvert the instrument, such as a smartphone, and turn it into a spy and tracking device for a jealous spouse, obsessed former associate or malicious voyeur.

The first major instrumented/interconnected/intelligent case before the U.S. Supreme Court involved a GPS tracking device. The Supreme Court of the United States found the placement and monitoring of a GPS tracking device on a person's automobile while it travelled on public roads to be illegal absent sufficient evidence relating the vehicle to criminal activity as determined by a neutral magistrate [1]. This was an "unreasonable search" even though it would have been completely permissible for police agents to follow the automobile in their own vehicle and log the movements.

Although a prevailing rationale was that the placement of the tracking device without permission was a trespass, Associate Justice Sonia Sotomayor in a concurring opinion addressed the growing risks pervasive computing and communications technologies, such as GPS-enabled smartphone presented for traditional notions of privacy. Electronic surveillance may still be improper "when the government violates a subjective expectation of privacy that society recognizes as reasonable" [2] and she agreed with Justice Alito that long-term GPS monitoring would impinge on those expectations.

But Justice Sotomayor continued in *United States v. Jones*,:

> In cases involving even short-term monitoring,... GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations... ("Disclosed in [GPS] data... will be trips the indisputably private nature of which takes little imagination to conjure: trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on"). The Government can store such records and efficiently mine them for information years into the future... And because GPS monitoring is cheap in comparison with conventional surveillance techniques and, by design, proceeds surreptitiously, it evades the ordinary checks that constrain abusive law enforcement practices: "limited police resources and community hostility." Illinois v. Lidster, 540 U. S. 419, 426 (2004).

The knowledge of such surveillance could have a negative impact on freedoms of speech and association with others as well as provide the government with immense private information subject to misuse.

Security is a global idea tied to safety, an assurance that a person may go about his or her life without injury to life, property or rights. Cyber security is a subset that focuses on computing systems, their data exchange channels and the information they process, the violations of which may be sanctioned under criminal law [3]. Information security and assurance intertwine with cyber security with a focus on information processed.

With computing systems the kernel of security concerns is the information handled by the system. The three general areas to be secured are

(1) The "privacy" and confidentiality of the information
(2) The integrity and authenticity of the information and
(3) The availability of the information for its use and services.

Further, the legal and social concepts of a citizen's "right to privacy" are entangled with the challenge of cyber security and the benefits of the Smart City. That legal/social concept of privacy addresses confidential aspects of life, control of one's own public profile and a life free of unwarranted interference. This applies to both state action and that of private parties.

Within most democratic and hybrid legal regimes under common law, civil law and mixed systems there are core general principles relating to privacy and cyber privacy:

(1) Activities within the home have the greatest level of protection and are generally protected from intrusion by others absent reasonable grounds and, often, judicial orders of intrusion, based on law.
(2) Activities that extend outside the home may still be protected as to privacy but the level of protection may vary. This may depend on whether there is a "reasonable expectation of privacy," [4] under U.S. constitutional law, or a special protection out by statute for that activity [5].
(3) Activities out in public or involving third parties may have little or no protection as to privacy absent special protection out by statute for that activity [5].
(4) Activities subject to public regulation may carry lesser or no privacy protections, particularly where data collection is part of regulation or a pre-condition to state permission to use regulated services [6].
(5) Any activity data may be monitored, collected and used with the consent of the data subject, absent statutory prohibitions on use even with consent. Third parties may condition use of their services or products on consent to such data use, even where a data subject may consent without actually reading the consent document they execute.

As to "cyber privacy" the legal regime is further defined by related, analogous statues that may prohibit unauthorized access to a computer, a network and related data, unauthorized

interception of, interference with or transmission of data and unauthorized data processing and analytics of a data collection [7].

Any of these may be authorized by statute, judicial order or the consent of a data subject.

So the data processes of the Smart City may be completely permissible under the law. But the benefits of the Smart City, such as locational services, may create unexpected risks.

Representation and modeling

We can represent the whole domain as some Sets and relations as follows:

The sets are mainly, the Persons (P), the Servers (S), and the Things (T) which are elements of the Internet of Things. Essentially, we have:

$$P = \{p_i, p_2, \ldots, p_L\}$$
$$S = \{s_1, s_2, \ldots, s_M\}$$
$$T = \{t_1, t_2, \ldots, t_N\}$$

where: M < L N since there are less servers than persons and much less persons than thing in the emerging Internet of Things.

The traditional Security and Privacy concerns are focused on protecting the vertices of the following within graphs:

$$G_p = \{P, E_P\};\ \text{where}\ E_P = \{(p_i, p_j)\}\ \text{such that}\ i, j = 1, 2, \ldots, L$$
$$G_S = \{S, E_S\};\ \text{where}\ E_S = \{(s_i, s_j)\}\ \text{such that}\ i, j = 1, 2, \ldots, M$$

The within graph of Things as listed here is currently ignored as it is not the focus of attacks

$$G_S = \{T, E_T\};\ \text{where}\ E_T = \{(t_i, t_j)\}\ \text{such that}\ i, j = 1, 2, \ldots, N$$

The external relation graphs representing interactions such as between persons-servers and person-things are represented below:

$$G_{PS} = \{P, S, E_{PS}\};\ \text{where}\ E_{PS} = \{(p_i, s_j)\}\ \text{such that}\ i = 1, 2 \ldots L, , j = 1, 2, \ldots, M$$
$$G_{PT} = \{P, T, E_{PT}\};\ \text{where}\ E_{PT} = \{(s_i, s_j)\}\ \text{such that}\ i = 1, 2 \ldots L, , j = 1, 2, \ldots, N$$
$$G_{ST} = \{S, T, E_{ST}\};\ \text{where}\ E_{ST} = \{(t_i, t_j)\}\ \text{such that}\ i = 1, 2 \ldots M, , j = 1, 2, \ldots, N$$

With the growing number of interconnected Things, G_{PT} and G_{ST} are becoming extremely important and almost intractable. Our focus in the near future will be on protecting the varices of these graphs to create secure and privately acceptable Smart Cities.

Results and discussion

Our first discussion is the impact of these issues relating to transportation. Intelligent transportation, public and private, has access to a web of interconnected data including financial, GPS, vehicle state (within various parameters), weather and traffic updates.

Though legal and social expectations of privacy are less in public, mobile and regulated environments, people still have expectations as to rights of privacy and information security in those environments. Those security and safety concerns may be enhanced because of danger from misuse or accident, misconduct of others.

As in other areas of social instrumentation, the evolution of the Smart City and computational transportation networks is evolving and growing. We examine and discuss those components within the IN3 and the Source-to-Use structures and the issues of security and privacy each presents as to the system of automobile transportation in the United States. Automobiles are data sources from a variety of subsystems within them that produce different types of information. These data are collected locally but may also be transmitted and collected in central repositories where it ay analyzed and used for a variety of purposes.

Instrumented transportation systems – sources of data and the data types

Automobiles and their systems may be a major source of various kinds of data about a person's activities. Within an automobile the various systems represent different data sources with different data types.

In the United States mandatory computational instrumentation of automobiles began in the mid-1990s with the requirement that new cars sold in the United States have On-Board Diagnostic computers (OBD II) to monitor engine and system activity. These data could be used to diagnose engine performance issues and behavior.

Other types of system instrumentation came into wider use. Event data recorders (EDR), sometimes referred to as "black boxes," are data recording devices that record and preserve various information on automobile recorded activities including OBD data. The National Highway Traffic Safety Administration of the United States (NHTSA) mandated the types of data EDRs must collect including the format of the data and its survivability [8].

Global Positioning Satellite (GPS) systems for location and navigation and devices for hands-free use of cellular telephone and messaging services have also become popular in vehicles.

Some of the sources and types of data these systems collect and store on the local instrumentation are:

OBD/EDR (Event Data Recorders) – speed, acceleration, braking, seatbelt usage, vehicle status, airbag deployment
Hands-free telephone and messaging – Telephone and contact numbers, messages, texts
GPS navigation systems – trip data, home site, backtrack data ("breadcrumb")

Security and privacy issues

For such instruments the privacy concerns relate to the data kept in them. Locational data can detail much about a person's life they do not wish revealed, as Justice Sotomayor discussed as to medical, political or social contexts. GPS systems can track destination and origination points when used and may even store the actual route taken. Access to contact lists and messages tells much that may need to be kept private for personal, professional or commercial reasons.

Locational data can be a key security concern. Many set the GPS originating address from their homes. Access to these data details that home location. If the automobile is away from home, that home may be a better target for burglary. If the

driver is avoiding a stalker, now the stalker knows where they live.

The OBD II systems are open access without sufficient security. OBD II Bluetooth dongles may be surreptitiously installed, allowing external monitoring [9]. Vehicles with native Bluetooth access may also be compromised.

The Event Data Recorders raise several issues [10]. Vehicle manufacturers have used EDR data in their defense against claims their vehicles were at fault in crashes [11,12]. Claims of surreptitious data collection as an invasion of privacy have been rejected. *Id.*

Legally these data are within the control of the vehicle owner who controls access to that data absent a judicial order to produce it to third parties, including the government. Accessing these data without consent or a judicial order is unauthorized access to a computing device that carries both criminal and civil penalties.

With these data from these sources, the next step is to collect that data via systems that offer remote viewing and remote analysis for many different purposes.

Internetworked transportation systems

Interconnection with other remote systems may enhance transportation features, from voice, messaging and security to enhanced maintenance and vehicle servicing. The two-way communications of mobile data services and the "telematics" of automobile instrumentation can speed a driver through a toll booth, alert to an accident, keep an eye on your teenager out driving and reduce your insurance rates by showing good driving habits. Some of those services and the data they collect are:

- GM OnStar service – data alert service, navigation, tracking, Stolen Vehicle Slowdown, Remote Ignition Block
- Chevrolet Volt monitoring and Nissan Carwings monitoring systems for the electric Leaf
- Supplemental OBD/EDR monitors for insurance, commercial and young drivers – e.g., Travelers IntelliDrive, Progressive Snapshot – that track location, speed, braking and other driving data.
- GPS monitors for commercial, public safety, young drivers – time, location data.
- Toll and fee transponders – ID, time, location data which may also be used for traffic data studies, tracking
- Bluetooth system access
- proposed OBD III transponder-assisted on board diagnostics for engine and emissions performance using roadside readers, satellite or local stations [13].

60% of cars worldwide should have connected capabilities by 2017, according to ABI Research [14].

General Motors controversially proposed to share its monitoring data with GM related third parties to offer maintenance and other services, including those who have not signed up for or continued OnStar services [15]. The negative response from the owners of GM vehicles, especially those that had discontinued the OnStar services and did not otherwise expect their driving data was being monitored, led GM to withdraw that proposal.

Toll transponder services offer the great convenience of letting drivers on through tolling stations, speeding their journey. But that transponder data is now also collected by traffic authorities for data studies on traffic activities. As the transponders identify the driver/vehicle for payment purposes, they provide time and location data points on drivers or vehicles of which the drivers may not be aware. To prevent this the devices must either be turned off or, as one suggestion, covered in a Faraday cage Mylar bag until needed for toll payments.

The availability of BlueTooth access to automobile systems brings the benefits and risks generally associated with BlueTooth. Inadequately secured ports may lead to system compromise, the danger of which depends on the automobile systems accessed via the BlueTooth port.

SEMA notes these concerns regarding the proposed OBD-III data collection, transmission and monitoring for analytics and use [5]. OBD-III imposes sanctions based on "suspicionless mass surveillance" of private property

- Random, possibly frequent testing
- No advanced knowledge vehicle will be tested
- Results of testing not immediately available (unless roadside pullover follows)
- No opportunity to confront or rebut
- Possible use of system for other purposes (Police pursuit/immobilization, tracking, cite speeders).

Intelligent transportation systems

Analysis of transportation data may further enhance efficiency and safety. Analytics against these data can support interventions that improve engine efficiency and reduce emissions. Traffic patterns and system utilization may be better understood for better roads planning, signal use and differential road use taxes.

Examples of such systems, data collected and analytical outcomes are:

- Analysis of telematics-based driving data – Progressive's Snapshot will analyze driving data (speed, braking, time of day, etc...) to predict risk of accident and resulting cost [5].
- Transponder traffic data studies
- Autonomous automobiles – Google driverless car.

Data analytics are massively powerful tools for modeling, visualizing and understanding human behavior. The impact has yet to be fully understood.

Telematic driving data is used in the United States and the United Kingdom take the collection of data as to a driver's speed, braking, acceleration, location and other factors and analyze it against historical data and patterns to predict who will have an accident.

They can predict the risk of accident and the potential cost such that better driving habits may be advised or introduced or differential rates may be applied to compensate for the increased financial risk.

In the United States early efforts to restrict data analytics across government databases had limited impact [16]. The

European privacy initiatives have had a greater impact restricting data processing against privacy rights.

The potential benefits of intelligent analysis of the mass of traffic data are huge. Safer and more efficient transport, driverless systems for the young, the elder and disabled and fairer distribution of costs for casualty.

A key issue will be privacy and a citizen's relationship with the state, as detailed by Justice Sotomayor, above. As central as transport is to modern life, such analytics will turn everything into a transparent world unlike anything in the modern world. Protecting privacy will require a combination of legal and technical security measures. Each alone will be insufficient.

But security and privacy are also vital to the personal safety and security of people and their families. The security issues with information in the Smart City extend to relations between the people of the city and their own personal safety. General crime theory is another way to consider these issues for the Smart City. One criminological theory for examining meta-security issues in the Smart City is Routine Activities Theory. Routine activities theory in crime control can map to information security and suggest vulnerabilities and solutions for enhanced IT security.

Felson et al. argued that three elements promote a criminal act: a motivated offender, a suitable target and the absence of a capable guardian [17,18]. The confluence of these elements in everyday activities increases the likelihood of crime; the absence of an element decreases it. This approach can be mapped to information security to suggest alternative approaches to information security.

Information security for the Smart City must examine the suitable targets of compromise and the consequences of that compromise. Those would be, most directly, information and the systems controlled by information. The information may relate to personal privacy or autonomy of individuals, or it may "intellectual property" exploited by a compromise, such as copyright, patent or trade secrets. The systems compromised may solely process the information or use it for control systems ranging from power grids to medical services.

Routine activities theory suggests, distributed security services and responsibilities. It delineates that three elements promote a criminal act: a motivated offender, a suitable target and the absence of a capable guardian. The confluence of these elements in everyday activities increases the likelihood of crime; the absence of an element decreases it.

The "motivated offender" class may be identified by motivations that extend from profit to sheer circumstance. Motivations may be singly or in multiples embrace temptation, provocation, available time and boredom. The "suitable target" is that object of opportunity for the offender and the facts for the calculus of success that an offender makes. Those facts considered include the ease of access to the target, the profit/reward it offers, the ability to avoid detection or "ease of escape," portability of the target and ease with which it is disposed of.

The presence of "capable guardians" refers to constant and present individuals whose presence deters misconduct or speeds recovery by repair or sanctions against offenders. Vital to this concept is that guardians are more than legal authorities such as police. It includes friends, good citizens, neighbors and parents whose moral suasion alone may deter misconduct. Such guardians may support the recovery from misconduct and assist legal authorities in the prosecution of those committing misconduct.

In its turn, information security addresses three general domains of prevention, detection and recovery from a security compromise. This applies generally to information systems, and particularly to computers, networks and the Internet. [Stallings] These goals may be secured through security services for data that assure confidentiality, authentication and integrity and access control and availability, like the ITU-T X.800 Security Architecture for OSI.

Digital objects, security domains and services and Routine Activities elements may be compared and mapped. For the Smart City the technical target and the related consequence, such as injury to property, personality, life or limb, must be viewed jointly as that, in turn, maps to the nature of the motivated offender and the potential guardians to block that offender.

In the context of transportation system motivated offenders may include juveniles, thieves, vandals and stalkers/domestic abuse perpetrators. The motivations range from boredom to malice to profit to madness.

Instrumented transportation systems offer suitable targets for an offender motivated stalking/domestic abuse.

First and foremost, the victim/target's privacy is heavily compromised in that access to vehicle systems provides the offender with near complete information on where, when and for how long the victim/target has visited a particular location. It may provide additional information on whom the victim/target called.

This privacy violation is a major security risk. Once the motivated offender has a profile and location on the victim/target at all times he or she knows when that victim/target would be most vulnerable to a physical attack.

Further, override of vehicle electronics themselves may offer opportunities for harassment or injury by such a motivated offender.

These systems and their use must consider what capable guardian services can mitigate these risks. Technical hardening of such systems is important, even as some early implementations do not seem to have anticipated these risks from even such vulnerabilities as open BlueTooth access ports. System implementation that both locks the data collected by these systems and notifies a vehicle user that the information is being transmitted/accessed are important security features. Capable guardians may include those who do vehicle maintenance or other instrumented data recipients who may alert the victim/target to compromise in the system that may appear in their data. And it must also include the user/target, who should not be left ignorant of these issues but should be informed of the vulnerabilities, risks and proper responses.

Conclusions

Matching the daunting security vulnerabilities Smart City systems may present in the hands of unwitting users is the absence of a clear theory of law and rights to define what can and should be done with the power these systems represent.

Justice Sotomayor suggested in her concurring opinion in the *Jones* GPS tracking case that a reevaluation of the concept of privacy and third party data collection should be undertaken in this new age of electronic data collection and analysis

[19]. Her concern, as seen simply in GPS data collection and analytics, was that:

> The net result is that GPS monitoring—by making available at a relatively low cost such a substantial quantum of intimate information about any person whom the Government, in its unfettered discretion, chooses to track—may "alter the relationship between citizen and government in a way that is inimical to democratic society" [20].

The good and the bad of this altered relationship may be seen in investigation of the 2013 Boston Marathon terrorist bombing in United States. The quick and wide distribution of information via social media and other multimedia systems aided in public engagement and the swift identification of the suspects, an association with possible motives and the apprehension of one suspect [21,22]. But it also led to false leads and injudicious actions by some wrongly accusing individuals and groups of the crime [23]. Some have come to question whether or not the untrained use of these interconnected, instrumented and unmediated social relations may have risks that outweigh the benefits [24–26].

These concerns are present in the discussions over the proper role of state security in legal monitoring and analysis of telecommunications transactional data, such as that over the proper role of the U.S. National Security Agency.

In sum, the benefits do and will far outweigh the risks when the rights and liberties in a democratic society are observed and protected. The Smart City offers us much. But we must not let it take that which makes us who we are. Difficult and concerted debate on these issues is needed.

Conflict of interest

The authors have declared no conflict of interest.

References

[1] United States v. Jones, 565 U.S. ___, 132 S. Ct. 945 (2012).
[2] Kyllo v. United States, 533 U. S. 27–33 (2001).
[3] Council of Europe CETS No. 185 Convention on Cybercrime, *opened for* signature Nov. 23, 2001, *available at* <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm> (accessed 24.04.13).
[4] United States v. Katz, 389 U.S. 347 (1967).
[5] 18. U.S.C. §2510, Electronic Communications Privacy Act, Part I 18 U.S.C. §2701, ECPA Part II.
[6] Gordon Daniel, Upside Down Intentions: Weakening The State Constitutional Right To Privacy, A Florida Story Of Intrigue And A Lack Of Historical Integrity, 71 Temp. L. Rev. 579 (Fall, 1998).
[7] Convention on Cybercrime of the Council of Europe; 18 U.S.C. §1030, the Computer Fraud and Abuse Act (US); European Privacy Directive.
[8] 49 CFR Part 563, Event Data Recorders, Tables I and II (US).
[9] Terence Eden, "Car Hacking – With Bluetooth OBD" June 12, 2012, <http://shkspr.mobi/blog/2012/12/car-hacking-with-bluetooth-obd/> (accessed 24.04.13).
[10] Patrick R. Mueller. Comment: Every Time You Brake, Every Turn You Make–I'll Be Watching You: Protecting Driver Privacy In Event Data Recorder Information, 2006 Wis. L. Rev. 135.
[11] Batiste v. General Motors Corporation, 802 So. 2d 686, 687–88 (La. Ct. App. 2001)
[12] Harris v. General Motors Corporation, 201 F.3d 800, 802 (6th Cir. 2000).
[13] OBD-III Frequently Asked Questions, SEMA, <http://lobby.la.psu.edu/_107th/093_OBD_Service_Info/Organizational_Statements/SEMA/SEMA_OBD_frequent_questions.htm>.
[14] <http://www.abiresearch.com/>.
[15] The Town Talk, Technology: Only you – and your care – know where you've been." May 24, 2013, <http://lobby.la.psu.edu/_107th/093_OBD_Service_Info/Organizational_Statements/SEMA/SEMA_OBD_frequent_questions.htm> (accessed 25.04.13).
[16] Brandon John, "Are drivers ready for Big Brother car insurance plans?" April 24, 2012, <http://www.foxnews.com/leisure/2012/04/24/are-drivers-ready-for-big-brother-car-insurance-plans/>.
[17] Cohen Lawrence E, Felson Marcus. Social change and crime rate trends: a routine activity approach. Am Soc Rev 1979;44:588–605.
[18] Felson Marcus, Clarke Ronald. Opportunity Makes the Thief: Practical theory for crime prevention, Police Research Series, Paper 98, Barry Webb, Ed., Policing and Reducing Crime Unit, Research, Development and Statistics Directorate, Home Office, United Kingdom.
[19] 5 U.S.C. §552, the Privacy Act of 1974 (US).
[20] United States v. Jones, 565 U.S. ___, 132 S. Ct. 945 (2012), concurring opinion of Justice Sotomayor.
[21] United States v. Cuevas-Perez, 640 F. 3d 272, 285 (CA7 2011) (Flaum, J., concurring).
[22] Voice of America, "Multi, Social Media Play Huge Role in Solving Boston Bombing, April 26, 2013m <http://www.voanews.com/content/multi-social-media-play-huge-role-in-solving-boston-bombing/1649774.html> (accessed 28.04.13).
[23] CBS News, "Social Media and the search for the Boston bombing susptects." April 20, 2013, <Computer Engineering and Computer > (accessed 28.04.13).
[24] Lance Ulanoff, Mashable Op-ed, "Boston Bombings: Truth, Justice and the Wild West of Social Media," April 28, 2013. <http://mashable.com/2013/04/18/boston-bombings-wild-west-of-social-media/>.
[25] Bensinger Ken, Chang Andrea, Los Angeles Times, "Boston Bombings: Socil media spirals out of control," April 20, 2013 <http://articles.latimes.com/2013/apr/20/business/la-fi-boston-bombings-media-20130420> (accessed 28.04.13).
[26] Jonathan Dyer, BBC Radio, "Social Media and the Boston Bombings," 27 April 2013, <http://www.bbc.co.uk/programmes/p017cr7p> (accessed 28.04.13).