Privacy in the Smart City—Applications, Technologies, Challenges, and Solutions

David Eckhoff and Isabel Wagner

***Abstract*—Many modern cities strive to integrate information technology into every aspect of city life to create so-called smart cities. Smart cities rely on a large number of application areas and technologies to realize complex interactions between citizens, third parties, and city departments. This overwhelming complexity is one reason why holistic privacy protection only rarely enters the picture. A lack of privacy can result in discrimination and social sorting, creating a fundamentally unequal society. To prevent this, we believe that a better understanding of smart cities and their privacy implications is needed. We therefore systematize the application areas, enabling technologies, privacy types, attackers, and data sources for the attacks, giving structure to the fuzzy term "smart city." Based on our taxonomies, we describe existing privacy-enhancing technologies, review the state of the art in real cities around the world, and discuss promising future research directions. Our survey can serve as a reference guide, contributing to the development of privacy-friendly smart cities.**

***Index Terms*—Smart city, taxonomy, privacy, types of privacy, status quo, privacy-enhancing technologies (PETS).**

I. Introduction

SMART City has become an umbrella term for numerous technologies with the goal of improving the efficiency of future cities and the quality of life for their inhabitants, not just by introducing new applications but also by making existing processes smarter. It has become fashionable to call cities *smart* and there are political efforts intended to encourage the development of smart cities [1]. There exist a number of formal definitions of what makes a city smart: Caragliu *et al.* [2] define "a city to be smart when investments in human and social capital and traditional (transport) and modern (ICT) communication infrastructure fuel sustainable economic growth and a high quality of life, with a wise management of natural resources, through participatory governance." While others argue that there cannot be an absolute definition as the term smart city does not describe a static concept but rather a process towards more liveable and resilient cities [3], there seems to be agreement that certain novel technologies and applications amount to making cities smarter [4].

Manuscript received November 20, 2016; revised May 14, 2017 and July 1, 2017; accepted August 28, 2017. Date of publication September 5, 2017; date of current version February 26, 2018. *(Corresponding author: David Eckhoff.)*

D. Eckhoff is with the Robotics and Embedded Systems Research Group, Technical University of Munich, 85748 Munich, Germany (e-mail: david.eckhoff@tum-create.edu.sg).

I. Wagner is with the Cyber Security Centre, De Montfort University, Leicester LE1 9BH, U.K. (e-mail: isabel.wagner@dmu.ac.uk).

Digital Object Identifier 10.1109/COMST.2017.2748998

The number of smart city applications is large, ranging from smart card services for easy authentication and payment on the go, to smart resource management of water or electricity, to smart mobility applications that improve traffic efficiency and reduce CO_2 emissions. The effectiveness of these and other smart city applications heavily relies on data collection, interconnectivity, and pervasiveness.

Unfortunately, this is also the reason why smart cities pose a major threat to the privacy of citizens: The collection and correlation of large amounts of data allows the creation of detailed profiles encompassing every aspect of life. For example, a smart card service may disclose purchase behaviors, a smart building may reveal which appliances are used, and a smart mobility application may leak location traces of its users. In addition, the overcollection of sensitive user data constitutes a business case [5] and is already a problem in smartphone applications [6].

The high level of interconnectivity further adds to the body of privacy problems. Combining multiple data sources from different data holders, devices, and applications can improve service quality and availability, but also increases the risk for leaks of sensitive data and privacy violations through correlation.

The pervasiveness of applications and sensors leaves the individual citizen no choice but to become a digital part of future cities. Contrary to social networks where users willingly disclose personal information, many smart city applications do not require or even allow the user to control what data is being collected or transmitted. This loss of data sovereignty is a concerning development because *opting out* of the smart city is infeasible for many.

To make things worse, privacy protection does not yet seem to be an integral part in current smart city development. Several rankings compare cities in terms of *smartness* [7]–[9] by assigning scores to dozens of indicators. Across the three rankings, only one indicator refers to privacy, particularly the presence of a privacy policy. Academic literature on privacy in smart cities is still scarce, and many reports intended for the creators of smart cities do not even mention the word privacy. For example, a case study on world-leading smart cities does not cover privacy [10], and even though a recent report on smart cities in the U.K. mentions privacy in passing, it does not acknowledge it as a general challenge or problem [11]. Readers of these reports – which are targeted at city leaders, vendors, service providers, and investors – could be led to believe that there are no privacy concerns in smart cities at all.

On the bright side, many studies have identified that user acceptance is one of the most important requirements for the successful introduction and operation of new smart city technologies [12]. The fact that user acceptance is strongly dependent on the level of privacy protection [13], [14] requires cities, corporations, and researchers to design privacy-protecting smart city applications. Privacy-friendliness can therefore play a key role in the success of new services or products.

The implementation of privacy protection is complicated by the complexity of the smart city landscape, in particular the diversity of applications, technologies, involved parties, privacy threats and existing protection mechanisms. Understanding these aspects and their interconnection is necessary so that engineers, stakeholders, and researchers can design a privacy-friendly smart city and avoid contributing to an Orwellian future.

Contributions: In this article, we systematize the overwhelming complexity of the smart city with a particular focus on privacy. Our main contributions are:

- We present taxonomies for (1) the applications a smart city may provide, (2) the technologies used to enable them, (3) the types of privacy affected by smart city applications, (4) the attackers, and (5) the sources of data attackers can use.
- We present an overview of building blocks for privacy protections, including strategies to incorporate privacy into system design, cryptographic techniques to protect sensitive data, and security considerations.
- For each enabling technology, we identify privacy threats and describe possible solutions. Where applicable we point to open research directions.
- We review examples of smart city applications that have already been realized in cities around the world and analyze which privacy protections have been deployed.
- We discuss research directions that could contribute to privacy protection in smart cities.

II. Taxonomies

In this section we present the taxonomies used throughout this article. First, we classify smart city applications and the technologies that enable them. These taxonomies are based on an extensive review of literature and the state of the art in the domain of smart cities. While the differentiation of various smart city applications seems to be a common approach, taking a closer look into the technologies that enable these applications can provide more clarity on where and how privacy is at risk. This allows the classification and structuring of current smart city research and development, however, we note that these taxonomies may need to be extended in the future when new application areas arise and new technologies become available.

We then present a taxonomy of privacy, dividing it into five types that show which kind of user information is exposed. Finally, we classify types of attackers in the smart city and the data sources through which they can compromise user privacy. Table I shows which attackers, data sources, and privacy types have already been shown to be applicable to each of the enabling technologies and points to relevant examples in the literature.

A. Smart City Applications

The overarching goals of smart cities are to improve their citizens' quality of life and to create economic growth. These two goals can be achieved by increasing efficiency and sustainability, by allowing citizens to participate, and by improving decision making through the increased availability of information. To this end, many smart city applications have been proposed or already been deployed in nine key areas: Mobility, Utilities, Buildings, Environment, Public Services, Governance, Economy, Health Care, and Citizens (see top half of Figure 1).

These nine areas are by no means isolated from each other. Rather, services in different areas can interact and are often deployed in conjunction. For example, smart buildings are often combined with smart utility solutions to enable grid-controlled electricity demand management [12], [15].

Smart Mobility: One of the features most associated with the smart city is a smart transportation system that improves traffic safety and efficiency, reduces the time citizens spend in transit and thus improves quality of life. The applications in this area cover both private and public transport: Intelligent vehicles are envisioned to introduce advanced driver assistance systems or even autonomous driving by the use of sophisticated sensors [16] and communication systems [17]. Smart, adaptive traffic lights can improve traffic flow and reduce travel times and CO_2 emissions [18]. Location-based services such as assistance systems for finding the nearest gas station [19], EV charging station [20], or free parking spots [21] (combined with dynamic pricing [22]) can reduce delays and improve traffic flows in the city. On a larger scale, traffic flow optimization during rush hours and public events [22] and bus route optimization [23] further contribute to increasing traffic efficiency. Finally, shared bike programs [10] and a network of cycling paths [22] can reduce car traffic and air pollution.

Smart Utilities: Smart utilities aim to reduce the consumption of resources such as energy, gas, and water and can thus contribute to economic growth, sustainability, and efficiency. Well-known examples for smart utility applications are smart grids, virtual power plants [12], and distributed energy storage [24]. These systems are usually enabled by installing smart metering devices [23] but can also incorporate decentralized electricity generation or even electric vehicles [25]. Other smart utilities include water monitoring and water pressure management [21], or the adaptive employment of both conventional and renewable power plants based on the current and projected electricity demand [24].

Smart Buildings: Smart buildings aim to make residential and commercial buildings both more energy-efficient and more convenient to live or work in. For example, smart buildings can monitor their own structural health [21], regulate lighting and heating based on presence detection [26], and use intelligent appliances to automate everyday tasks [15], [27]. The field of home automation, also known as the *smart home* [28],

TABLE I
THE MOST COMMON ATTACKERS AND DATA SOURCES FOR EACH ENABLING TECHNOLOGY, AND THE PRIVACY TYPES THAT ARE DIRECTLY AFFECTED BY THE TECHNOLOGY (WE DO NOT INCLUDE PRIVACY TYPES THAT ARE AFFECTED BY CORRELATION WITH OTHER DATA)

	Attackers			Data Sources			Privacy Types				
	Service Providers	Involved Parties	Third Parties	Repurposed Data	Observable Data	Published Data	Body & Mind	Location	Media	Behavior & Action	Social Life
Ubiquitous Connectivity	[63]	[64]	[65]	[63]	[65]		[63]	[63]	[65]	[63]	[65]
Smart Cards	[66]			[66]				[67]		[67]	
Open Data	[68]		[69]			[70]	[71]	[71]	[69]	[72]	
(Participatory) Sensor Networks	[29]	[40]	[73]	[40]	[73]			[73]	[13]		
Wearable Devices	[74]		[75]	[74]	[75]		[76]	[77]	[78]	[77]	
Internet of Things	[47]	[79]		[47]			[48]	[80]	[81]	[80]	[82]
Autonomous Systems	[83]		[84]	[84]	[84]		[84]	[84]	[84]	[85]	
Intelligent Vehicles	[86]	[87]	[88]	[86]	[88]	[89]		[88]	[90]	[88]	
Cloud Computing	[91]			[81]			[47]	[22]	[81]	[81]	[82]

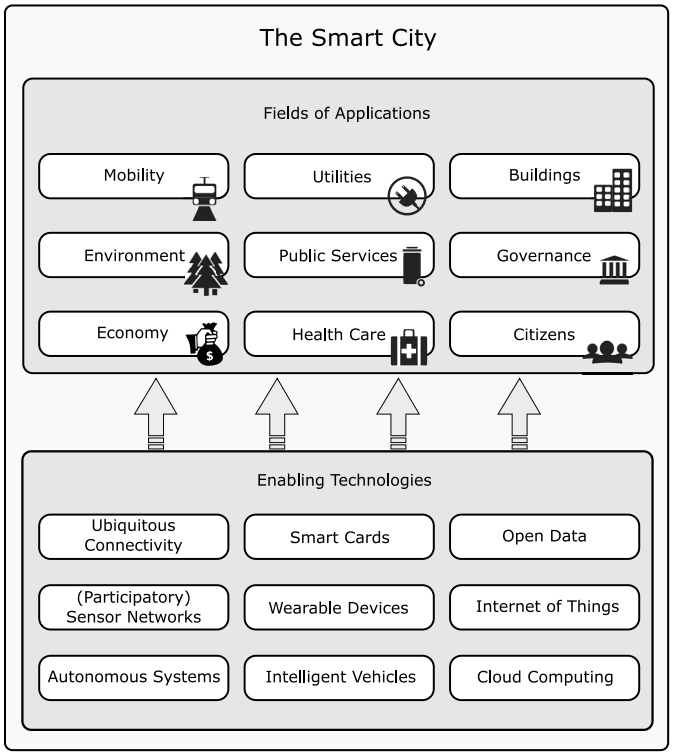


Fig. 1. Smart city applications and enabling technologies.

has experienced a noticeable increase in popularity lately. A number of connected sensor and actuators work together to improve the home's energy efficiency and introduce new comfort features.

Smart Environment: Smart environments aim to improve the sustainability of cities and the quality and safety of citizens' lives, e.g., by the creation of noise and air pollution maps [21], [22], [26]. This enables the timely detection of unhealthy or hazardous conditions and allows the authorities to react accordingly, for example, by limiting traffic in an affected area, warning citizens, or even evacuating entire areas of the city [29]. Further, sensor networks can detect natural disasters such as earthquakes, volcanic eruptions, tornadoes, floods, and forest fires [21], [30]. Early warning systems can significantly contribute to limiting casualties and reducing property damage. Ideally, these systems work together with other aspects of the smart city such as smart transportation to control traffic flows out of the city or smart utilities to shut down power plants in the hazard zone.

Smart Public Services: The goal of smart public services is to deploy public resources efficiently and effectively. Applications include adaptive waste management, for example by optimizing routes for waste collection [22] or the installation of smart trash cans that send alerts when full [23]. Crisis response and management applications can make resources and data such as building plans available to first responders [31]. The timeliness and effectiveness of public safety services can be supported by distributed sensing systems such as connected cameras [27] or audio monitoring systems [13]. Other examples include smart street lighting that adapts to movement of cyclists and pedestrians to increase traffic safety and improve energy efficiency [32].

Smart Governance: Smart governance tries to increase transparency, improve the efficiency of local government, and tailor government services to its citizens. For example, open data enables citizens, third-party developers, and the city council to access and cross-reference different data sources [20], which can increase both transparency and efficiency. E-government services allow citizens to complete most interactions with government services online, e.g., when booking weddings or applying for social housing, resident parking permits, or schools [10], [33]. Citizen participation allows individuals to get involved in city planning and development processes, for example through apps to report problems, virtual community meetings [10], and online portals for citizens to propose improvements to their city [20].

Smart Economy: A smart economy aims to create economic growth, for example through public-private partnerships [22] and new business models such as recommender services [34].

New business models are also based on the increasing availability of open data [10] and the drive to integrate data from different sources [12]. Cities can encourage entrepreneurship by supporting office spaces for startups, creating collaborative spaces and entrepreneur networks [20], and by offering affordable broadband connectivity [10].

Smart Health Care: Smart health includes the efficient and effective provision of health care. For example, smart medical centers can combine patient health records from multiple sources and thus improve medical care [23]. Smart health care can also rely on data from connected medical devices [32] and wearables [35]. Citizens can receive treatment via tele-health to reduce waiting and travel times [6]. Lastly, smart health care aims to empower patients by granting them access to their own health records and information about their conditions [10].

Smart Citizens: Finally, smart cities aim to invest in people to create smart citizens [32] and smart communities [34]. For example, smart education uses life-long learning programs [22], which may focus on employability [11], digital inclusion [10], or specific population groups, e.g., children with autism [36]. Subsidized broadband connectivity can support citizens in disadvantaged neighborhoods [10], and interactive information poles can give citizens and tourists access to various services [23].

B. Enabling Technologies

The novelty and innovation in the smart city does not primarily lie in the applications but in the use of underlying technologies that enable them. Based on our literature review, we grouped technologies commonly associated with the smart city into nine categories: Ubiquitous Connectivity, Smart Cards, (Participatory) Sensor Networks, Wearable Devices, the Internet of Things (IoT), Intelligent Vehicles, Autonomous Systems, Cloud Computing, and Open Data (see bottom half of Figure 1).

These technologies in turn were made possible by other technological progress. To name a few, embedded systems have significantly expedited pervasive and ubiquitous computing. Smaller and faster microprocessors allow complex tasks to be computed by portable devices or even home appliances. Energy-efficient computing as well as long-lasting batteries extend the lifetime of mobile devices and exterior sensors. Lastly, radio technology such as passive RFID tags and microstrip antennas have made it possible to equip even the smallest items with communication capabilities, making them a potential part of the interconnected smart city.

Most smart city applications rely on a combination of two or more of these enabling technologies. For example, a combination of participatory sensor networks and ubiquitous connectivity enables city-wide real-time monitoring of noise and air pollution which contributes to a smarter environment.

Ubiquitous Connectivity: A connection to the Internet is a requirement for many services that incorporate user devices such as smartphones, tablet computers, smart appliances, or intelligent vehicles. In urban areas, most homes are already equipped with landline broadband Internet and the coverage of high speed cellular networks such as 4G is swiftly increasing. With small enough cells and new technologies such as 5G, mobile Internet should be able to fully support emerging smart city applications [37].

There are, however, reasons for users to choose a WiFi-based Internet connection over a cellular link. Often, cellular Internet plans come with a limit in data volume, therefore transferring large media files is not an option. Other users, such as tourists from other countries, might not have a cellular Internet plan and fully rely on other possibilities to connect to the Internet. In these cases, projects to offer free Internet connections using public WiFi, possibly provided by the city, shops, or even private user groups, can offer a viable alternative to cellular Internet access.

Smart Cards: Modern smart cards enable the transmission of authentication data, function as cashless payment methods, or even serve as driver's license and travel documents [38]. While smart cards have been around for decades, contact-less smart cards and the interconnection of smart card readers enables many new applications. Most current smart cards are based on the ISO/IEC 14443 family of standards [39]. They have writable storage, a microprocessor, and use a transmission technology similar to RFID for short range communication. Many smart card applications can operate offline, requiring the smart card to hold all of the necessary data which is then accessed by a smart card reader/writer. The smart card readers can also be connected to a back-end server to allow additional security and accounting features.

Open Data: Open data refers to data that is publicly available (technical openness) and may be used and analyzed by third parties (legal openness). Open data can increase government transparency and foster innovation by allowing third parties to offer services based on city data. Cities can use open source platforms like CKAN to release data [22].

(Participatory) Sensor Networks: Sensor networks are the basis for many applications in the smart city, ranging from smart public services to smart buildings and environments, to smart mobility. They can be seen as knowledge collectors providing the data necessary for (possibly automated) informed decisions and actions. Examples include fire detection or air pollution monitoring, but also CCTV systems and induction loops (when connected to a central traffic control center). Cities aim to increase sensor coverage and availability to monitor every aspect of the city. Sensor networks in smart cities can also include the sensing capabilities of citizens' devices such as smartphones. This is referred to as *participatory sensing*, *crowd sensing*, or *opportunistic sensing* [14], [40]. Location-based services are another application enabled by sensors, particularly the availability of small receivers for satellite-based positioning systems like GPS, GLONASS, and GALILEO.

Wearable Devices: In contrast to data generated by sensor networks, the data from wearable devices or body area networks is almost always personal data specific to the wearer. The devices monitor different aspects of the body, e.g., blood pressure, heart rate, or even brain activity [41]. Equipped with communication technology, these readings can then be transmitted to medical practitioners, contributing to smarter health care. Wearable devices may not only be used in a hospital environment with extensive body monitoring, but also

in other areas such as private homes, e.g., to monitor vital signs of patients with chronic illness. The American Federal Communications Commission has already allocated a dedicated spectrum for both use cases [42]. At the same time, wearable devices for recreational use, such as smart watches and fitness wristbands, are rapidly gaining popularity. Other types of wearable devices include smart glasses and contact lenses [43] that can augment reality to interact with smart city applications and technology. Smart nanotextiles, featuring sensing, actuation, and communication capabilities, will further contribute to the pervasiveness of health and environmental monitoring [44]. A person's wearable devices can be connected to form a so-called body area network to provide additional features such as data aggregation and fusion as well as the possibility for low-energy devices to interact with the smart city though a gateway node, e.g., the wearer's mobile phone.

Wearable devices could also be incorporated to access smart city services, e.g., by conveniently displaying information or by using the device to interact with readers. They could further be envisioned to serve as sensors and be integrated as a part of a greater (participatory) sensor network.

Internet of Things (IoT): The IoT is "a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies" [45]. The IoT thus describes the equipping of common objects with communication devices (often connecting to big data services), sensors, and actuators [46]. While conceptually similar to sensor networks, the difference in the IoT is that the sensing and communication capabilities are not the main feature of the object, but an extension to improve operation or provide additional services. Popular examples include smart meters [47], the smart fridge [48], and smart air conditioning systems [49].

Autonomous Systems: Autonomous systems, often in the form of robots, will play an important role in future cities. For example, autonomous vehicles have the ability to dramatically change the way people travel by shifting from car ownership to shared autonomous vehicles [50]. Autonomous systems can also carry out tasks for the city, such as delivery of goods, street cleaning or waste collection, and can even extend to surveillance using autonomous drones [51].

Intelligent Vehicles: Intelligent vehicles are vehicles equipped with a range of sensors, communication capability, or the ability to drive autonomously. They can exchange information in an ad-hoc fashion, inform infrastructure nodes such as traffic lights and dynamic traffic signs, or access centralized services like traffic information or emergency services using cellular technology. The ad-hoc communication based on IEEE 802.11p has already been standardized in North America and Europe [52]. Furthermore, the introduction of autonomous taxis and ride sharing systems can have a significant impact on city mobility [53]. Because the average vehicle is parked 23 hours a day [54], these systems offer a large potential to reduce the overall number of vehicles.

Cloud Computing: Cloud computing refers to the outsourcing of computational tasks to third parties, which provide either the hardware infrastructure, the operating system platform, or entire software applications as a service [55]. Cloud computing turns the one-time cost of purchasing IT hardware into a running cost that depends on service consumption. Cloud services can scale quickly and efficiently to the level of user demand that a cloud customer experiences. In a smart city, this is useful to ensure availability of public-facing Web services or to scale the amount of data analysis done on data gathered throughout the city.

C. Five Types of Privacy

Almost every aspect of a citizen's privacy is potentially at stake in a smart city because smart city applications pervade the very space in which citizens live. Privacy has been established as a human right in Europe and is often referred to as "the right to be let alone" [56]. This rather generic definition, however, is hard to adapt to today's technology where large amounts of private data are collected, processed, and stored. This makes defining privacy difficult. Solove [57] even stated that "privacy a concept in disarray" and that "nobody can articulate what it means." Without a clear definition of privacy violations, it becomes impossible to safeguard privacy and develop privacy protection mechanisms. The definition by Nissenbaum [58] produces relief by defining privacy as contextual integrity. This concept has found wide adaptation and can serve as a general guideline when dealing with sensitive data. Following contextual integrity, the expectations regarding data collection and dissemination are determined by the social norms in a particular context. For example, in the context of a doctor's visit, one expects that only relevant medical data is collected, and that the data is not shared outside of the doctor's practice. Any use or collection of data outside of these expectations constitutes a privacy violation.

To better understand the privacy at risk in a specific scenario, different authors have introduced taxonomies for privacy [57], [59]–[61]. For example, Clarke introduced four types of privacy in 1997 [59], that is, privacy of the person, personal data, personal behavior and personal communication. Finn *et al.* [61] argue that the advance in technology demands that these categories be extended and divide privacy into seven types, namely privacy of person, thoughts, behavior, communication, association, data and image, and location.

However, we argue that these categories are not defined clearly enough and make some unnecessary distinctions. We therefore propose three changes to the categories defined by Finn *et al.* First, communication with another person always includes some form of association, meaning that the communication and association category can almost not be separated. Therefore we merge them into the privacy of social life category. In fact, we believe that communication should not be a separate privacy category, as it is more of a medium, that, when compromised, can be exploited to learn every aspect about a person. Technologies that can compromise communication should therefore not be limited to only this one category as this would be an underestimation of their privacy implications.

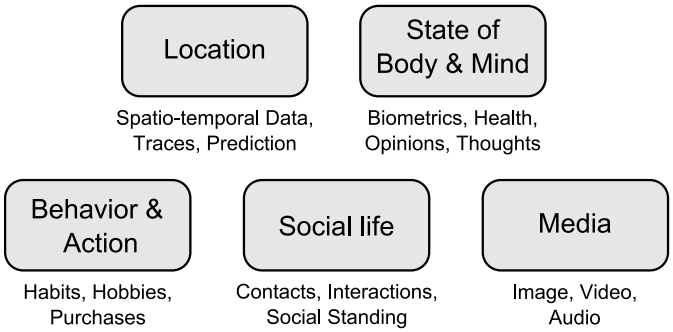


Fig. 2. We define 5 types of privacy to classify privacy risks introduced by different smart city applications and technologies.

Second, the privacy of data and image category is both too general and too specific at the same time. Personal data can include information about every other privacy category, and without sensitive data, there can be no privacy violation. We therefore remove this aspect and change this category to privacy of media to not only include images, but also other types of media, such as audio or video.

Lastly, Finn *et al.* [61] split Clarke's category of privacy of the person into privacy of the person and privacy of thoughts and feelings. They state that emerging technologies have the potential to learn about a persons thoughts and feelings and that these categories should be distinguished "the same way that the mind can be distinguished from the body". However, research in neuroscience and neurophilosophy increasingly concludes that mind and body are indeed not separate [62]. Both privacy of a person and privacy of thoughts cover aspects specific to an individual. These are characteristics that are not necessarily associated with being in a certain location or with carrying out certain actions. We therefore combined these privacy aspects in the privacy of state of body & mind category.

Our five types of privacy (see Figure 2) can thus be described as follows:

Privacy of Location: Location information does not only include the location itself but also when and for how long it was visited. Location privacy is usually defined as the protection of spatio-temporal information. Violating location privacy can reveal a person's home and workplace, but also allow inferences about other types of privacy, for example habits, purchase patterns, or health [34]. In addition, co-location information allows inferences about a person's social life.

Privacy of State of Body & Mind: The state of body and mind encompasses a person's bodily characteristics including biometrics, their health, genome, mental states, emotions, opinions, and thoughts. Violating the privacy of the state of body and mind can lead to discrimination by employers and insurance companies or even to prosecution by totalitarian regimes.

Privacy of Social Life: A person's social life includes the contents of social interactions, for example what was said in a conversation or posted on a social media platform, as well as metadata about interactions, for example who a person interacts with, when, and for how long. Violating social privacy allows inferences about other types of privacy, e.g., interactions with specialized hospitals or political groupings can reveal information about a person's health or opinion.

Privacy of Behavior & Action: The privacy of behavior and action includes a person's habits, hobbies, actions, and purchase patterns. When shopping online or when using credit cards, potentially intimate details are shared with retailers. Exploiting this information for other purposes such as targeted advertisement can constitute a violation of privacy. Often, this information allows to draw far-reaching conclusions about the user's life and therefore other types of privacy.

Privacy of Media: Media privacy includes privacy of images, video, audio, and other data about a person [13]. This includes CCTV and other (knowingly or unknowingly taken) camera footage or media uploaded to the Internet. Redistributing or creating user-related media without consent constitutes a privacy violation.

D. Attackers and Data Sources

Privacy protections in smart cities need to be designed and implemented with different attackers in mind. Metrics to measure the privacy enjoyed by users in a system heavily depend on the type (and capabilities) of an attacker [92], [93]. Attackers can be defined using orthogonal dimensions [94], [95]: they can be internal or external, passive or active, global or local, and static or adaptive. Their capabilities can vary in terms of resources (e.g., network coverage, computational power), the employed algorithms (e.g., restriction to algorithms with probabilistic polynomial time), and also depend on the level of prior knowledge and available information (e.g., information from a side channel or scenario-specific knowledge). This classification is useful when investigating a specific attack or when measuring privacy properties such as anonymity [94], but is overly specific when discussing general privacy threats for a broad area such as the smart city. We therefore focus on the attacker's role in the smart city and distinguish Service Providers, Involved Parties, and Third Parties (see bottom half of Figure 3).

Service Providers: Service providers include utility companies collecting smart meter readings, providers of location-based services, Internet service providers, cloud computing services, and the government. They have direct access to the data collected by their services and may have incentives to repurpose this data.

Involved Parties: Involved parties include device manufacturers (for example of wearables, smart cards, vehicles, or CCTV cameras), software developers, and other users who can authenticate to the system but may behave maliciously. Involved parties may gain access to potentially sensitive data.

Third Parties: We refer to all entities that are neither a service provider nor involved with the infrastructure and devices as third parties. They include external attackers who may not be able to authenticate to the system but acquire data through other channels.

Attackers in smart city scenarios can use four sources of data to attack privacy: Observable Data, Repurposed Data, Published Data, and Leaked Data (see top half of Figure 3).

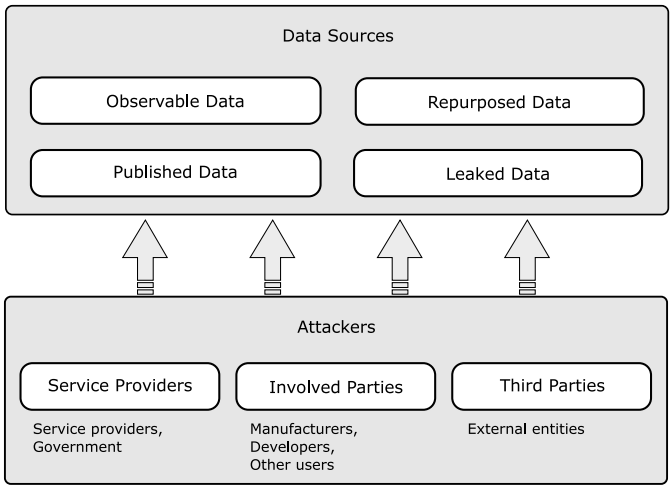


Fig. 3. Attackers and data sources used by attackers.

Attacks based on Observable Data: Observable data can be acquired by eavesdropping on wireless and wired communication. The attacker is passive, but needs to be present at a physical location where the communication can be overheard.

Attacks based on Repurposed Data: Repurposed data has been collected for a specific purpose, but is then repurposed for a different cause. The attacker could be a service provider, for example for location-based services, who uses user data not only to provide the service, but also to profile users. According to contextual integrity [58], repurposing data without user consent always constitutes a privacy violation.

Attacks based on Published Data: Published data is available to the public. This includes statistical data from open government platforms as well as data that individuals choose to reveal. The attacker can correlate published data with other data to infer information about individuals.

Attacks based on Leaked Data: Leaked data was intended to stay private, but has been obtained by the attacker, for example through software flaws, security vulnerabilities, misuse of authorized access, or social engineering. These leaks have been common in the past and should therefore be expected [96]. However, the implications on privacy can be severe if this data is not protected, and the consequences for data holders include large fines and a loss of reputation. Perfect protection is unlikely, however, a combination of the privacy technologies we present in Sections III and IV can considerably decrease the impact and risk of a data leak.

III. Building Blocks for Privacy Protection

In this section, we briefly review key building blocks for privacy enhancing technologies (PETs) that have been developed over the past decades. Because smart city applications combine a range of enabling technologies, it is plausible that existing privacy mechanisms for these enabling technologies can be reused in the context of smart city applications. We will refer back to these technologies from Section IV, when we discuss privacy challenges and solutions for smart cities, and we will outline open issues and challenges in Section V.

PETs are used to achieve or protect certain privacy properties. The *type* of privacy that PETs protect depends on the context in which they are used, for example location privacy in smart mobility, or privacy of body & mind in smart health. In contrast, *privacy properties* as defined by Pfitzmann and Hansen [60] are independent of the context. They define six key privacy properties: anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management. Anonymity means that a subject is not identifiable within a set of subjects; unlinkability refers to the property that two actions or individuals cannot be linked by an attacker; undetectability means that an attacker cannot sufficiently distinguish whether an item of interest exists; unobservability requires undectectability and the anonymity of all involved entitites; pseudonymity is the use of pseudonyms as identifiers instead of real names; and identity management refers to managing of partial identities, such as pseudonyms. In addition to these six properties, PETs often provide confidentiality to ensure that message contents cannot be read by unauthorized parties.

A. Process-Oriented Privacy Protection

We begin with privacy techniques that address the process of developing and operating privacy-friendly systems and are thus applicable to most technologies.

Privacy by Design: Privacy by design is often mentioned as a strategy to fix privacy issues in smart cities [13], [15], [22]. Privacy by design encompasses seven principles that should be followed [97]: proactive privacy protection instead of remedial action after privacy violations have happened; privacy as the default setting; privacy embedded into the design; full functionality with full privacy protection; privacy protection through the entire lifecycle of the data; visibility and transparency; and respect for user privacy. However, this definition of the privacy by design principles is quite vague and sometimes circular [96]. In addition, [98] argues that privacy by design – in the form of Privacy Impact Assessments – needs to be legally mandated (instead of relying on voluntary compliance) to "protect the core values of our Western liberal democracies and constitutions."

Nevertheless, there have been attempts to incorporate these principles into the design of new systems. For example, [99] uses two principles, proactivity and end-to-end security, to guide the design of a remote health monitoring solution, and [100] apply the transparency principle to intelligent transport systems. Gürses *et al.* [96] argue that, although not explicitly listed in the seven principles, data minimization should be the core of privacy by design. We discuss data minimization as a data-oriented privacy protection in the next section.

Privacy Requirements Engineering: To apply privacy by design to the smart city in a *systematic way*, the principles need to be incorporated into a privacy engineering process. For example, the process proposed in [96] starts with functional requirements analysis and data minimization, then considers attackers, threats and additional security requirements, and finally implements and tests the design. To incorporate

privacy requirements into a standard software engineering process, [101] proposes eight privacy design strategies. Four strategies concern *data* (minimize, hide, separate, and aggregate), and four strategies concern *process* (inform, control, enforce, and demonstrate).

Privacy considerations can also be integrated into a formal requirements engineering process. For example, PriS is a privacy requirements engineering method that can be used on top of an existing goal modeling method (e.g., Enterprise Knowledge Development (EKD), KAOS, or Secure Tropos) to elicit a smart city's privacy requirements [102]. To identify privacy goals, PriS starts from the privacy properties defined by Pfitzmann and Hansen [60] and proposes privacy-enhancing technologies that satisfy each of the properties.

LINDDUN is another privacy requirements engineering method that has been defined in analogy to STRIDE [103]. LINDDUN defines a list of privacy threat types (and is named after their initials: linkability, identifiability, non-repudiation, detectability, disclosure of information, content unawareness, policy and consent noncompliance), most of which correspond to the privacy properties defined in [60]. LINDDUN then maps these privacy threat types to elements of the system model, aided by a library of threat tree patterns and a mapping of privacy-enhancing technologies to privacy goals.

Reference [104] compares PriS, LINDDUN, and Spiekermann's Framework for Privacy-Friendly System Design [105], and finds that they can be mapped to a common conceptual framework that helps to select the most suitable requirements engineering method.

Testing and Verification: An important part of privacy-friendly system design is privacy testing and verification to ensure that the design and implementation of a system do indeed fulfill its privacy requirements. According to MITRE, privacy testing is not fundamentally different from other types of testing and thus needs to be incorporated into existing testing processes [106]. Testing approaches that are specific to privacy requirements aim at finding information leaks from applications, for example through black box differential fuzz testing [107] or taint tracking, i.e., analysis of the information flow of sensitive program inputs to program outputs [108], [109]. The privacy properties of cryptographic protocols can also be formally verified using formal languages such as the applied pi calculus [110], using ontologies [111], or using model-based approaches [112].

Transparency: Transparency concerns the issue that data accumulates in the hands of governments and corporations, while individuals neither know what data is being held about them, nor can they exert control over their data [113]. To increase transparency, the provider should openly communicate what data is collected, what data is stored, how it is processed, who it is shared with, and how it is protected [15]. For example, cities could send citizens monthly reports of the data held about them [114], and integrate this data report with an easy way for citizens to correct or delete their data. Transparency may increase the level of trust for the citizens [115] and thereby increase acceptance of smart city applications.

Transparency also includes algorithmic transparency [116], that is, openness about the algorithms used for data processing. Algorithmic transparency can increase the level of perceived privacy by explaining, in easily understandable ways, how potentially privacy-invasive systems work. This applies to almost every technology in the smart city, such as how smart card data is processed, or how autonomous systems make decisions.

Consent and Control: Consent is an important stipulation for lawful data processing [32]. However, in a smart city environment, traditional methods of acquiring consent may break down. For example, users cannot review the privacy policies of smart dustbins they pass on the way to work [32], and there are no buttons to disable ambient audio monitoring [13]. In a similar way, it can be difficult to give users control, that is, the right to view, update, and delete data held about them [101] because citizens may not even be aware that there is data held about them.

Another aspect of control is to ensure that data is handled according to each user's privacy settings [12]. This type of control can be realized using information flow control, which allows to track the usage of sensitive data throughout an application and has been implemented, for example, for Android phones [109]. Policies on information flow can be enforced, for example by trusted hardware [117].

Auditing and Accountability: Accountability in smart cities has two different meanings: First, to hold the city accountable for its use of citizen data and compliance with its privacy policies, and second, to hold citizens accountable for misbehavior, e.g., to make sure that citizens pay the correct amounts for usage of public transport, toll roads, or energy.

Logging and auditing allow the smart city to demonstrate that it complies with its privacy policies [118], [119]. This encompasses the ability to determine when privacy breaches have taken place, and which records are affected [101]. Independent audits also allow the public to understand how, and how often, privacy-invasive technologies are being used, whether they are being used for their stated purpose and how well they fulfill this purpose [120].

Citizen accountability is supported by several data-oriented privacy protections which we discuss in the next section.

Privacy Architectures: Privacy architectures are needed to tie different protections together and ensure that there are no privacy leaks at any point. For example, the architecture in [121] relies on trusted remote data stores and a broker that mediates access to the users' data stores. Similarly, [12] uses a broker to provide access control for centralized storage, and [122] combines different cryptographic techniques to provide privacy guarantees.

B. Data-Oriented Privacy Protection

Data Minimization: As discussed above, data minimization can be derived from the privacy by design principles [96]. In smart cities, data minimization has already been used to formally analyze architectural choices for electronic toll pricing [123] and to derive privacy-preserving solutions for big data analysis [124].

A specific challenge to data minimization is that the sensors of modern smart systems naturally gather more sensor data than required for the envisioned task. We refer to this data as *collateral data*. For example, cameras for specific tasks such as face recognition or traffic surveillance also record unrelated information, e.g., two persons holding hands or a person limping. The system should therefore be designed to limit the recorded data for the envisioned use case to avoid exploitation.

Data Anonymization: k-Anonymity is a popular technique aimed at preserving the privacy of individuals in public releases of statistical databases by providing anonymity and unlinkability. The key idea is that databases, for example with medical information, contain both identifying information (e.g., the names of individuals) and sensitive information (e.g., their medical conditions). Assuming that columns with identifying information are removed before publication, k-anonymity then groups the database rows into equivalence classes with at least k rows that are indistinguishable with respect to their quasi-identifiers [125], [126]. Quasi-identifiers by themselves do not identify users, but can do so when correlated with other data. For example, the combination of the three quasi-identifiers ZIP Code, date of birth, and gender identifies 87% of the American population [126]. Each equivalence class contains all rows that have the same values for each quasi-identifier, for example all individuals with the same ZIP Code, date of birth, and gender. To ensure that all equivalence classes have at least k rows, several algorithms have been proposed to transform a given database to make it k-anonymous, for example using suppression or generalization [125] or random sampling [127].

However, k-anonymity has been shown to have shortcomings that allow re-identification of individuals and/or their sensitive information in several situations, for example with high-dimensional data, multiple releases of the same database, or when correlations with other data sources are possible. For this reason, many variations of k-anonymity have been proposed, for example l-diversity which ensures that sensitive values are well-represented in each equivalence class [128], m-invariance which can deal with multiple data releases [129], or t-closeness which restricts the distribution of sensitive values [130] (see [131] for a good survey of the most important variations).

Differential Privacy: Differential privacy is a more modern approach to database privacy that can provide unobservability. In contrast to k-anonymity, differential privacy can give privacy guarantees: any disclosure is equally likely (within a small multiplicative factor ϵ) regardless of whether or not an item is in the database [132]. For example, the result of a database query should be roughly the same regardless of whether the database contains an individual's record or not. This guarantee is usually achieved by adding a small amount of random noise to the results of database queries. Originally introduced for interactive database queries, differential privacy has since been extended to many other settings, for example non-interactive data publishing [133], smart metering (and stream data in general) [134], and location privacy [135].

Encryption: Encryption preserves privacy by protecting the confidentiality of messages or other data. Traditionally, symmetric encryption requires two parties to have a shared en-/decryption key, while public-key encryption allows to encrypt messages using a public key, and only the corresponding private key can decrypt the messages.

Identity-based encryption is a type of public-key encryption where the public key can be an arbitrary string, such as a user's name or email address [136]. This allows to encrypt messages for a recipient even if the recipient has not generated a public/private key pair. Identity-based encryption can be used to realize private service discovery [137].

Attribute-based encryption is another type of public-key encryption where both the private keys and the ciphertexts depend on user attributes [138]. A user is only able to decrypt a message if his key's set of attributes matches the ciphertext's set of attributes. In this way, fine-grained access control on encrypted data can be realized. In smart cities, attribute-based encryption can be used to encrypt data for several groups of recipients who share common attributes, such as doctors, nurses, and patients [139], [140].

Homomorphic Encryption: Homomorphic encryption (HE) is a cryptographic method that allows computations on encrypted data and thus protects confidentiality during data processing. For example, the addition of two ciphertexts representing the encrypted numbers 2 and 3 would result in a ciphertext representing the encrypted number 5. Partially homomorphic cryptosystems are computationally feasible today, but they only allow either addition (e.g., the Paillier cryptosystem [141]) or multiplication operations (e.g., the ElGamal cryptosystem [142]), but not both. Fully homomorphic cryptosystems do not have this restriction, but are still computationally expensive [143], even though there has been significant progress in the past years [144].

The appeal of homomorphic encryption in smart city applications is that it can be used to allow third parties to process sensitive data without getting to know the inputs or outputs of the computations. For example, HE has been used to design privacy-preserving solutions for smart metering [79], genomic tests [145], and recommender systems [146].

Zero-Knowledge Proofs: Zero-knowledge proofs [147] are a cryptographic method that allows one party (the prover) to prove their knowledge of some fact to another party (the verifier), without revealing the fact or any other information [148]. Zero-knowledge proofs ensure that a cheating prover who does not know the fact cannot convince the verifier (the soundness property), and that a cheating verifier does not learn any other information (the zero-knowledge property).

Zero-knowledge proofs provide confidentiality and privacy-preserving accountability. For example, they can be used for authentication, allowing the user to prove that they know the password without revealing it. They also allow to enforce honest behavior, for example to prove that the steps of a protocol were followed correctly. This has already been used to design solutions for smart metering [47], [149] and electronic toll pricing [150].

Secret Sharing: Secret sharing is a method that allows to distribute secret information among several participants [151]. Typically, the secret is split into n shares, each participant receives one share, and a minimum of t shares is required to

recover the secret. Thus, secret sharing provides both confidentiality (a single share does not allow recovery of the secret) and reliability ($n-t$ shares can be lost without affecting recovery).

In smart cities, secret sharing can be used in solutions for data aggregation (e.g., from participatory sensor networks [152] or smart meters [153]), for distributed data storage [154], and for decentralized enforcement of k-anonymity [155].

Anonymous/Pseudonymous Digital Credentials: Anonymous digital credentials provide a privacy-preserving way for individuals to prove facts about them, for example whether they are a legitimate sender or have a specific attribute such as age or nationality, without revealing their identity.

For blind signatures, an authority signs messages without being able to read the message contents [156]. In this way, the authority attests that it has verified the message author's identity, but the signature does not reveal this identity. In smart cities, blind signatures have been proposed to verify that messages were sent by legitimate vehicles, without revealing the vehicle identities [157].

Anonymous credentials [158] allow users to obtain credentials from authorities and use these credentials while ensuring that transactions cannot be linked to each other or to the user. Attribute-based credentials rely on anonymous credentials and add features for revocation and de-anonymization [159]. Attribute-based credentials have many potential uses in smart cities, for example to allow users to authenticate with cloud providers without revealing their identities [19].

Pseudonymous credentials can be realized using a public-key infrastructure. The certificate authority issues a long-term certificate and a pool of pseudonymous certificates to each user. The long-term certificate is only used to obtain pseudonyms from the certificate authority to prevent re-identification of users. Pseudonyms are used for communication with other users and are only valid if signed by the certificate authority. Thus, receivers can check the validity, but not the identity of other users using the certificate authority's public key, and only the certificate authority can link pseudonyms to user identities. In smart cities, pseudonymous credentials are used in the industry standards for intelligent vehicles [88], [160] to ensure that drivers enjoy location privacy while still being accountable for their actions in traffic.

To improve privacy protection, the certificate authority can be separated into two entities, one for issuing long-term certificates and one for issuing pseudonyms. This is similar to direct anonymous attestation (DAA) [161] where each participant obtains a certificate from the DAA issuer. When receiving a message, the receiver contacts the DAA verifier who uses zero-knowledge proofs to verify the sender's credential. DAA thus requires the active participation of the certificate authority in every communication or transaction.

Anonymous and pseudonymous credentials provide anonymity and pseudonymity, respectively, as well as unlinkability. Both methods can allow authorities to de-anonymize users, thus providing accountability.

Secure Multi-Party Computation: Secure multi-party computation is a cryptographic method that allows two or more parties to jointly compute the value of a public function without revealing the parties' private inputs, and without relying on a trusted third party [162]. Secure multi-party computations provide confidentiality and unlinkability. They are computationally expensive, but real-world applications have already been reported, for example to realize auctions where the final price can be computed without revealing individual bids [163].

In smart cities, secure multi-party computations can be used to design healthcare solutions, for example to compute the results of genomic tests where both the patient's genome and the test sequence remain private [164].

Private Information Retrieval: Private information retrieval allows clients to query database servers without revealing the query or the query results to the server. Private information retrieval provides confidentiality, unlinkability, and undetectability. The simplest method to achieve private information retrieval is for the server to send the entire database regardless of the query. If servers are computationally bounded or if there are multiple non-colluding servers holding copies of the database, several protocols have been proposed that achieve private information retrieval at a lower communication cost [165]. In smart cities, private information retrieval can be used to hide access patterns to data stored in the cloud [166], [167].

C. No Privacy Without Security

Security and privacy are closely related terms and effective privacy protection is almost impossible without security. This article focuses on conceptual privacy challenges and solutions in smart cities. For example, a public camera placed to record and transmit images of individuals is a privacy problem by design, whereas failing to safeguard the communication of the camera to the back-end server is a security problem that leads to a privacy problem. The line between conceptual and security-related privacy challenges is blurred and therefore it is short-sighted to talk about privacy protection without outlining the security challenges of smart city technology. In this section, we give a brief overview of security challenges and problems that are of interest for most of the discussed smart city technologies.

The list of guidelines and principles to design secure computer systems is long and certainly out of scope for this article. We refer the reader for challenges specifically for embedded systems, and therefore for many smart city devices, to [168]. Here, we briefly review some of the most important concepts.

System security and access control: Privacy protection in the smart city often depends on the security of the systems and subsystems within it. For example, if attackers can compromise smart home devices, they can spy on the inhabitants or even gain physical access to the home (see [169] for a survey on security issues of the smart home and smart grid). This is not a conceptual privacy problem of the smart home idea, but a consequence of flawed or nonexistent security measures. This problem can be observed for many smart city technologies, including the IoT, wearable devices, sensor networks, autonomous systems, and intelligent vehicles, especially when these devices support a wide range of protocols and include

many software components. This is naturally the case for mobile phones that, when compromised, can lead to a complete violation of user privacy (see [64] and [170] for surveys on mobile phone security and privacy). The fact that users can actively download third-party software onto the devices furthermore opens up the problem of malware [171].

The sensory interfaces of many smart devices also pose a security challenge. It has been shown that the sensory channel of cyber-physical systems can be used to infect devices with malware [172], which can then be used for privacy violations. Similar attacks have been illustrated in the scope of intelligent, autonomous vehicles where LiDAR and other sensors can be influenced to affect short-term and long-term driving decisions of the cars [173].

Access control restricts access to stored data to authorized individuals, for example city employees [12], [15], [68]. While access control is necessary, it does not prevent the misuse of authorized access. Besides traditional access control for unencrypted data, attribute-based encryption also enables fine-grained access control for encrypted data [138]. Information flow control can track data as it flows through a system and enforce the data owner's access policies [174].

Access control is especially important for autonomous systems with an Internet connection through which devices can be compromised and remote-controlled. Unlike a compromised fridge where the worst case damage seems manageable, the actuators (wheels, grapplers, etc.) on modern robots allow an adversary to carry out a wide range of tasks that can cause damage to property and to persons [84].

Protocol and network security: Cryptographic protocols, for example, to establish a secure confidential communication channel, make use of cryptographic primitives, e.g., cryptographic hash functions or encryption algorithms. Although these primitives might be unknown to be susceptible to any feasible attack, an improperly designed protocol based on them may be [175]. This is challenging in terms of privacy, because just as these primitives are building blocks for security protocols, the security protocols are building blocks for privacy protection. If the underlying security architecture can be compromised, then privacy is at risk through an attack based on leaked data (see Section II-D). The impact can only be mitigated by carefully designing the system in a privacy-aware manner (see Section III-A).

Even without security problems, flaws in communication protocols can lead to privacy issues. For example, it has been shown that the 6LoWPAN stack includes header information that can be exploited to locate the device or even track activities of the user [176]. Hence, each system building on flawed protocols may leak information beyond what it has been designed for. Developers of a smart city applications should therefore always check whether the entire protocol stack supports the envisioned privacy goals.

Information leakage: Side channels, such as timing or power consumption, can leak information even if a system is secured by cryptography. These side-channel attacks can lead to privacy violations, e.g., when analyzing the communication of smart meters [177], IoT devices [178], or intelligent vehicles [179]. Location inference attacks can also use side channels (e.g., smartphones accelerators [180] or radio frequency fingerprinting [181]) to identify the location of a device or user. In general, the problem of a system revealing more information than intended needs to be carefully considered in the context of smart city technology, as every piece of information may be used by an attacker to break the security and privacy of the system.

IV. Privacy Challenges & Solutions

The complexity and number of smart city applications, technologies, and attackers make it hard to keep track of the privacy risks for citizens. It is often not the application itself that poses a risk but the way an application uses the underlying technologies. For example, cashless payment methods for public transportation do not constitute a privacy risk *per se*, but can be implemented in a privacy-invading way, for example by using smart cards that transmit identifying information (e.g., "Card holder is John Doe, 65, holds a severely handicapped pass, and has visited locations A and B earlier today"). We therefore structure this section along the nine enabling technologies in our taxonomy (see Figure 1, p. 491). For each technology, we discuss privacy issues, privacy-friendly solutions, and give examples how the technology is already used in real cities.

Table II shows which data-oriented privacy protections have already been applied to the enabling technologies and outlines how each solution preserves privacy. Missing entries in this table do not imply that these mechanisms are generally infeasible for a given technology, but only that we are not aware of literature applying the mechanism in the given context. Table III summarizes the examples of real smart cities we give in this section, as well as their applications, potential privacy issues, and what privacy protections are in place. We also give a (naturally subjective) rating how well privacy protection was addressed in each case.

A. Ubiquitous Connectivity

4G connectivity is already widespread in today's cities, and many cities are supplementing paid-for 4G connectivity with free WiFi access. Ubiquitous connectivity can be a privacy risk because (1) mobile Internet providers can track their users via cell tower and hot spot locations, (2) providers can read unencrypted user traffic, and (3) third parties can eavesdrop on the wireless channel.

Privacy for the Communication Channel: Traffic over public hot spots is not necessarily encrypted and can thus be monitored by the access point, all intermediate nodes, and other people in the vicinity. For example, [65] found that more than two thirds of airport WiFi users leaked personal information through name resolution queries, HTTP content, and profiled advertisements. From a smart city provider's perspective, this privacy leakage can be countered by offering encrypted wireless communication (e.g., WPA2), and securing all Web services and mobile apps using SSL/TLS. Even though the use of SSL/TLS is common, erroneous usage of the protocol can cause privacy leaks, for example due to lacking certificate validation [182], [183]. Erroneous usage can be

TABLE II
EXAMPLES OF HOW PRIVACY-ENHANCING TECHNOLOGIES HAVE ALREADY BEEN APPLIED TO SMART CITY TECHNOLOGIES

PET	Technology	Privacy-Preserving Solution
Data Minimization	Ubiquitous Connectivity	Use minimal permissions for mobile apps, avoid use of third-party libraries [64]
	Smart Cards	Do not store identifiers of smart cards [203]
	(Participatory) Sensor Networks	Isolate sensors from other systems, optimize placement to collect no PII [13]
		Extract relevant features on sensor, discard raw data [204]
		Separate entities that ask for and receive sensor readings [40]
	Wearable Devices	Reduce time and location granularity on device [205], [206]
		Extract relevant features on device, discard raw data [78]
	Internet of Things	Process data for smart metering on device, discard raw data [47], [149]
	Intelligent Vehicles	Process data for toll pricing on device, discard raw data [150]
		Require cooperation of multiple entities to de-anonymize vehicles [207]
Data Anonymization	Ubiquitous Connectivity	Change device identifiers frequently to prevent fingerprinting [194], randomize browser fingerprints [195], insert cover traffic [196]
	Open Data	Release only data that satisfy k-anonymity[126], l-diversity [128], m-invariance[129], or t-closeness [130]
	(Participatory) Sensor Networks	Ensure k-anonymity of sensor readings [155]
		Ensure spatio-temporal readings cover at least k individuals [73], [208], [40]
		Use l-diversity [128] or hierarchical map quantization [209] to prevent location semantics attacks against k-anonymity
	Internet of Things	Cluster IoT data streams and only release clusters with at least k members [210]
Differential Privacy	Open Data	Release noisy aggregates of data [211], e.g., public transport data [212]
	(Participatory) Sensor Networks	Obfuscate locations with planar Laplace noise [135], [213]
	Internet of Things	Apply noise to meter readings [134]
Encryption	Ubiquitous Connectivity	Ensure correct usage of SSL/TLS with static analysis [184]
		Ensure correct usage of SSL/TLS with dynamically linked libraries [185]
		Secure public WiFi with WPA2 [65]
		Use anonymous communication to protect metadata [186], e.g. Tor [187]
	Wearable Devices	Avoid storing encryption keys on device [214]
		Use cryptographically enforced role-based access control [215]
	Internet of Things	Use identity-based encryption for private service discovery [137]
	Cloud Computing	Use attribute-based encryption for access control [139], [140]
Homomorphic Encryption	(Participatory) Sensor Networks	Aggregate sensor readings from multiple participants privately [216]
	Internet of Things	Aggregate data over multiple participants [79], e.g. energy consumption [217]
	Cloud Computing	Privately process data at third parties [143]
Zero-Knowledge Proofs	Internet of Things	Enforce honesty of device for local processing, e.g., for smart meters [47], [149]
	Intelligent Vehicles	Enforce honesty of vehicle for local processing, e.g. for electronic tolling [150]
Secret Sharing	Open Data	Use privacy-preserving data aggregation [218]
	(Participatory) Sensor Networks	Enforce k-anonymity of sensor readings cryptographically [155]
		Compute statistics over sensor readings from multiple participants privately [152]
	Internet of Things	Aggregate data over multiple participants privately [153], [217]
	Wearable Devices	Use secure distributed data storage [154]
Anonymous/Pseudonymous Credentials	Smart Cards	Authenticate users without identifying them [219], [159]
	Intelligent Vehicles	Use short-lived pseudonyms for car-to-car communication [160], [220], [221]
		Preserve backwards-privacy when revoking pseudonyms [222], [89]
		Eliminate mapping between short-term and long-term identifiers [157]
	Cloud Computing	Authenticate users based on attributes instead of identities [19]
Secure Multi-Party Computation	Cloud Computing	Process data with private inputs [223], e.g. genomic tests [164]
		Perform privacy-preserving data mining over distributed datasets [224]
Private Information Retrieval	(Participatory) Sensor Networks	Ensure query privacy in location-based services [225]
	Cloud Computing	Hide access patterns to remote files [167]
		Hide access patterns to remote databases [166]

detected by static analysis tools [184], and validation can be improved with dynamically linked validation libraries [185].

Privacy for Metadata: Ensuring the confidentiality of communication content is not sufficient to ensure privacy, because the communication metadata (who communicates with whom, when, and how long) needs to be protected as well. For example, the fact that a patient communicates with a particular physician may reveal certain health issues. This risk can be mitigated by using specialized protocols, for example to hide the connection between patient and physician [186], or by using Onion Routing (e.g., Tor) [187] as a general-purpose tool for anonymous communication. However, the required technical knowledge to properly operate these tools may make them inaccessible for a majority of citizens. A possible way to overcome this problem is to have pre-installed and pre-configured software packages on smartphones or computers, and to generally increase the awareness of this privacy challenge, possible solutions, and the existence of easy-to-use integrated browser solutions. Unfortunately, even anonymous communication protocols may leak private information through various attacks [188], for example traffic correlation [189] or timing attacks [190].

Fingerprinting: Even when public Internet is used anonymously, fingerprinting techniques using static MAC addresses, browser and system parameters [191], clock skew [192], or frame inter-arrival times [193] allow to track and re-identify

TABLE III
EXAMPLES OF ALREADY DEPLOYED SMART CITY APPLICATIONS WITH POSSIBLE PRIVACY ISSUES AND PRIVACY COUNTERMEASURES (RATED AS NO/UNKNOWN ○, SOME ◐, AND GOOD ●)

City	Technology	Smart...	Application	Possible privacy issues	Privacy measures	Rating
Hong Kong	Ubiquitous Connectivity	Public Services	Free WiFi access	Browsing history and location tracking	WPA2 encryption, user activity is recorded and available to authorities	◐
Hong Kong	Ubiquitous Connectivity	Public Services	Companion app HK GovWiFi	Profiling through phone permissions: network access, location, phone identity + storage	No information about privacy policy	○
Chicago	Ubiquitous Connectivity	Public Services	Free WiFi access	Browsing history and location tracking	No encryption, no information about privacy policy	○
Estonia	Ubiquitous Connectivity	Public Services	Free WiFi access	Browsing history and location tracking	Mandatory data retention	○
Hong Kong	Smart Card	Mobility	Octopus card	Data about public transport usage and purchases	Data has been sold to marketers in the past	○
Zaragoza	Smart Card	Mobility, Citizens	Citizen card	Linkability of individuals to their card use	Privacy policy, but no information about privacy technologies	◐
Malaysia	Smart Card	Citizens	Compulsory citizen card MyKad	Card number leaks information about user	No information about access control	○
Almere	Open Data	Governance	StraatKubus	Presents sensitive data about individuals	Privacy impact assessment and access control	●
The Hague	Open Data	Environment	City dashboard	Data about emergency calls	Reason for emergency call is not included	○
Sydney	Open Data	Economy	Tap-on tap-off data	Data about public transport usage	Differential privacy	●
Chicago	Open Data	Health	Aggregated health data on city map	Sensitive health information about individuals	k-anonymity	●
Glasgow	(Part.) Sensor Networks	Mobility, Gover-nance	Operations center	Combination and automated analysis of CCTV footage	Compliance with UK data protection law, no information about privacy technologies	◐
Rio de Janeiro	(Part.) Sensor Networks	Environment, Gover-nance	Operations center	Combination of CCTV footage	No information about privacy protection	○
Glasgow	(Part.) Sensor Networks	Public Services	Intelligent street lights	Location tracking	Sensors detect presence, but not individuals	●
Eindhoven	(Part.) Sensor Networks	Environment	Stratumseind: people counting and noise monitoring	Location tracking, audio surveillance	Local data processing, no recording or transmission of raw data	●
Oulu	Wearable Devices	Citizens	App to track running data	Location tracking	Tracking only enabled during runs	◐
Copenhagen	Cloud Computing	Mobility	WiFi hotspots for traffic flow and safety	Location tracking	Information is aggregated and anonymized, but no technical information available	◐
Aspern	Internet of Things	Utilities, Buildings	Smart grid	Profiling via energy consumption	User consent, user engagement	◐
Zwolle	Internet of Things	Utilities, Buildings	Smart grid	Profiling via energy consumption	Data minimization, aggregation, and separation of knowledge	●
Bristol	Internet of Things	Economy	Wireless mesh and sensors on street lamps	Location tracking and audio surveillance	No information available	○
California	Autonomous Systems	Public Services	Surveillance robot Knightscope K5	Profiling, video and audio surveillance	Wireless communications are encrypted, otherwise no privacy protection	○
Waseda, Japan	Autonomous Systems	Citizens	Teaching robot Pepper	Profiling of children	No information available	○
EU	Intelligent Vehicles	Mobility	eCall automatic emergency calls	Location tracking	Basic eCall: tracking only when accident detected. Additional services: tracking possible	◐
Japan	Intelligent Vehicles	Mobility	Collaborative cruise control, intersection collision warning	Location tracking	No information about privacy protection	○

users. Protections against website and device fingerprinting include changing device identifiers frequently [194], randomizing browser fingerprints [195], and inserting cover traffic [196]. However, protections against physical-layer identification of wireless devices are still underexplored [197].

Privacy for Mobile Devices: The use of mobile devices for ubiquitous connectivity also brings privacy challenges. Modern mobile devices are equipped with a multitude of sensors which in principle allow for the pervasive monitoring of users. In addition, these devices consist of various components

developed by different parties with different goals and incentives, which makes the protection of sensitive user data more difficult. As a result, existing privacy solutions often focus only on a small part of the mobile device ecosystem and thus leave the user vulnerable [64].

For example, the baseband processor which is needed for cellular communications runs a separate operating system (in addition to Android or iOS) that most users do not know about. The baseband processor has access to the phone's microphone and often also to the phone's main memory. Together, these can be used for remote audio surveillance and reveal a user's location and private data [198].

Privacy risks are also introduced through the use of third-party applications. Even though both Android and iOS employ permission models to restrict the data that third-party apps can access, apps often request more permissions than necessary, and users often grant permissions that are more far-reaching than expected [199]. We refer the reader to a recent survey by Spensky *et al.* [64] for a more detailed discussion of these issues.

State of the Art Examples: Hong Kong offers free WiFi access at more than 600 locations in the city [63]. The WiFi is accessible to everybody without prior registration, and a public username and password is used for WPA2 encryption. However, the government reserves the right to record and analyze a log of activities for each user, including their browsing history. These records can be requested by law enforcement. The corresponding app *HK GovWiFi* asks for full network access, location, phone identity, and full access to the phone's storage.

Chicago, IL aims to increase Internet accessibility by providing free WiFi at a number of public places, low-cost fiber access, and subsidized Internet access in underprivileged residential areas [200]. Chicago's WiFi is open and not secured, and therefore accessible to everybody. However, we were not able to find information about the privacy policies of the free and subsidized services in Chicago. In particular, it is unclear whether a user's browsing history will be recorded.

The country of Estonia also offers free WiFi access at many public places. However, even though the Estonian constitution enshrines a right to privacy, Estonian law requires Internet Service Providers to store communications metadata, including the user's browsing history, for one year [201].

Projects to increase connectivity have also been initiated by communities and commercial Internet service providers. Community-driven mesh networks can provide connectivity for citizens who cannot afford it, and serve as a resilient network in case of emergencies [202].

B. Smart Cards

The main privacy issue in smart cards is the logging of transactions. For example, transactions in public transport can disclose spatio-temporal information about the card holder. These mobility patterns can include locations, habits, and visits to sensitive places or events. When data from different users is correlated, possible links between them can also be revealed. Information collected by smart cards can contribute to optimizing public transport schedules, however, it can also be repurposed for advertising, profiling, and tracking.

Separation of authentication and service: Separating user authentication from the service accessed by the user is a step towards providing unlinkability between users and transactions [219]. In some cases, this separation can be achieved by not including identifying information on the smart card, i.e., by using anonymous, pre-paid smart cards. In other cases, for example when the smart card is used to access buildings or to buy discounted bus tickets, the user needs to be authenticated to ensure that they are allowed to access the service. Even in cases where authentication is required, it is not necessary to create a link between user and transaction. Instead, attribute-based credentials allow the system to cryptographically verify certain of the user's attributes (for example, a *student* or *discounted fares* attribute would indicate that the user is entitled to discounted bus fares) without revealing the user identity [159].

Data minimization: The separation of authentication and service alone does not guarantee privacy because service data is often sufficient to re-identify individuals, for example the origin-destination pairs collected from a public transport smart card can reveal a person's identity [226]. This can be addressed by minimizing the amount of data collected and stored. The card's unique identifier can allow tracking and re-identification of users and should therefore not be stored [203]. In transportation, it is often sufficient to know the departing public transport zone instead of the exact bus stop to determine the price for a bus ride. Also, dynamic pricing can be done without a connection to a back end server, minimizing the collected information about each user. If fine-grained information is needed to optimize transport schedules, the system could instead record counts of passengers getting on/off at each stop.

State of the Art Examples: In Zaragoza (Spain) the *tarjeta ciudadana* (literally "citizen card") [20] aims to integrate services and make it easier for citizens to interact with city infrastructure. The Zaragoza smart card serves as photo ID, member card to access different city services, and payment method. Among others, the card can be used to access and/or pay for the public bus system, car parking, sports centers, municipal WiFi, museums, and libraries. The city asserts that no personal data is stored on the card. However, if a citizen ceases to be registered with the city of Zaragoza, the card will automatically be declined at public facilities. To realize this function, the card id has to be checked against an authentication/authorization server that links the card id to the citizen, even if the card itself does not store personal data. For payment, the card can be both pre- and post-paid. In the latter case, it requires citizens to have an account with a cooperating bank. Information on privacy and data protection from the public-facing website of the Zaragoza city council [227] states that (1) data is stored by the city council with the purpose of creating and managing the citizen card, (2) data is not shared with third parties except where necessary to provide the card services, (3) the council can cross-reference data generated by the card with other municipal databases, and (4) citizens have the right to access, correct, and delete data held about them.

However, there is no information regarding the extent of data stored or the names of third party providers. In addition, there is no public information about specific privacy technologies used.

In Hong Kong, the Octopus card allows users to pay for transportation, parking, and shopping [22] and gain access to buildings, schools, and hospitals. The Octopus card collects personal information about its users and card usage. The privacy policy permits use of the collected data not only for management and operation of the card, but also marketing [67]. In 2010, Octopus confirmed that it had sold information about 2 million customers to third parties [66], and claimed that doing so had not violated their terms and conditions.

In Malaysia, the MyKad smart card goes even further in that it serves not only as a compulsory national identity card, but also as driver's license, health card, transit card, and debit card [228]. In addition, many other applications use MyKad for authentication, for example schools, theme parks, and businesses. The MyKad number leaks the holder's date/place of birth and gender, and it is unclear whether access control to information on the card is enforced effectively [229].

C. Open Data

While traditional open government platforms publish data related to government activities, smart cities can collect a large amount of data about citizens which should not be published as-is because open data should not allow to identify individuals. However, simply removing all personally identifying information is not a sufficient protection against de-anonymization. For example, it has been shown that the combination of ZIP Code, date of birth, and gender uniquely identifies 87% of the U.S. population [126], and that high-dimensional data, such as a database of movie ratings, can be linked back to individuals by correlating it with other (public) data [72].

Aggregation: The publication of aggregated data can reduce privacy concerns. Data can be aggregated over time periods, individuals, or geographic areas. Aggregation is most effective if the raw data is hidden even from the service provider, which can be achieved by using cryptographic protocols, for example based on homomorphic encryption [218] (see also Section III-B and references in Sections IV-D and IV-F).

Obfuscation: Similarly, the publication of obfuscated data, i.e., data that has been sanitized through generalization, suppression, or randomization, can also reduce privacy concerns. For example, k-anonymity ensures that each individual's record is indistinguishable from at least $k-1$ other records [125], and several enhancements of k-anonymity have been proposed to mitigate its vulnerabilities [131] (see also Section III-B).

In contrast to k-anonymity, differential privacy can give privacy guarantees by adding noise to the results of database queries [211]. While originally introduced for the interactive setting (answering database queries), it has since been expanded to cover data publication and data streams [230].

State of the Art Examples: Almere (The Netherlands) operates the data platform StraatKubus which provides geographical information on the street level, including personal data such as household income, age ranges, rent arrears, and school failures. The purpose is to allow social workers and police to spot problem areas early on. To comply with privacy regulations, Almere created a detailed privacy impact assessment ("Gedragsrichtlijn") that explains the purpose of data collection for every goal of the StraatKubus and details how data may be stored and processed. As a result, only employees of the municipality can access the data, and only if they need it to perform specific tasks [68].

The Hague (The Netherlands) aims at creating an open data platform incorporating data about safety and liveability [68]. The city dashboard of The Hague [70] – and of many other cities in the Netherlands – features live updates on recent ambulance calls and fire alarms which include street address, priority, and timestamp. This data is based on messages on the unencrypted P2000 network, the dispatch system for all emergency services in the Netherlands. A number of websites exist which link the information in P2000 messages with maps and street views [71]. This has already led to privacy violations of the individuals requesting emergency services. So-called photo cowboys listen to P2000 messages to arrive early at emergency scenes to take photographs. Despite this, a 2013 initiative to encrypt P2000 messages was unsuccessful and one representative of a photo cowboy organization claimed that "the argument of privacy is nonsense" [69] because the P2000 messages do not include the reason for the emergency.

Sydney (Australia) has an open data policy that requires government data to be open by default, subject to appropriate privacy policies and "management of privacy for the individual". In a recent example, two weeks of tap-on tap-off data for public transport in Sydney were published. The data release states that "the tap on and tap off counts are not linked and individual trips cannot be derived using the data," and that the release uses differential privacy in combination with time and geographical aggregation [231]. According to a separately published technical report [232], the parameters for (ϵ, δ)-differential privacy were $\epsilon = 8$ and $\delta \approx 2^{-20}$. However, the value for ϵ is considered to be rather large, and due to small application errors, the data may still leak information about the presence or absence of individuals in specific circumstances and with low probability [212]. Even so, the combination of using state-of-the-art privacy protection and publishing both algorithm details and parameters is very good practice.

The Chicago Health Atlas publishes health-related data, for example statistics about common conditions, health insurance, hospital admissions, and demographics. The data is available on a neighborhood level (approx. 16 city blocks) and can be downloaded, displayed on a map, and plotted in time series plots that compare a neighborhood with the city-wide average. Before publication, the data has been anonymized to ensure that no individuals can be identified from the data. Although there is no public information about the method of anonymization, [233] suggests that the Chicago Health Atlas used k-anonymity with $k = 5$, and applied both generalization

(age ranges, aggregation of geographic areas) and suppression (no data about rare diseases with less than 5 patients) to achieve *k*-anonymity.

D. (Participatory) Sensor Networks

Sensors have become a ubiquitous technology, pervading both public and private environments. Unlike environmental sensors (e.g., in forests or the ocean), sensors in the smart city monitor the very space citizens live in and may thus collect sensitive data. CCTV systems, possibly coupled with facial recognition or automatic number plate recognition, enable the provider to track individuals throughout the city. Even seemingly noncritical systems like occupancy sensors that control light and heating in an office can reveal when an individual is at work. Location-based services such as parking spot finders disclose not only spatio-temporal user data, but also user queries. The notion that individuals implicitly consent to being monitored when moving in public space is worrying because the lack of alternatives means that consent cannot be meaningfully withheld.

Data Minimization: Personal information collected by sensors can be minimized by isolating sensors from other systems to avoid combination and correlation, by deleting personal data, and by optimizing sensor placement so that no personal information can be collected [13]. For many purposes of sensor data collection, it is sufficient to extract relevant features on the sensor and discard raw data to avoid collection of collateral data. For example, face verification for access control can be realized in a privacy-friendly way by extracting feature vectors from faces and comparing them to stored feature vectors [204]. In this way, no video data is stored, preserving the privacy of bystanders and reducing the inferences that can be made from clothes and personal appearance.

Aggregation: The privacy of participants in sensing applications can be protected by aggregating sensor readings over multiple participants. In many use cases, including smart buildings [208] or traffic monitoring [234], statistical information about sensor readings (e.g., average, count, or histogram) is sufficient to fully realize the application's purpose. These statistics can also be computed privately without a trusted third party using secret sharing [152] or homomorphic encryption [216].

Location Cloaking: The concept of *k*-anonymity (see Section III-B) can be applied to location privacy by using as quasi-identifiers the location and the time of the reading or user query [73]. For example, in the case of occupancy sensors, spatio-temporal cloaking can be achieved by dynamically adjusting the size of the reported area and the time granularity until the reading covers at least *k* individuals. This can be achieved by a trusted anonymity server [73], by relying on collaboration between all sensors [208], or by private information retrieval which can guarantee privacy for continuous queries without relying on a trusted third party [225].

In a participatory sensing system, achieving *k*-anonymity is more challenging, as the reporting user devices cannot always communicate with each other. An entry is then *k*-anonymous if the report could have been generated by at least *k* other devices. To achieve this, the size of the area can be precomputed using a tessellation approach based on empirical data [40]. Mobile devices reporting a location will then replace the location in their reading with the coordinates of the polygon to statistically ensure their reading is *k*-anonymous. The downsides of this method are that devices require a common data-set of a potentially fast changing environment and that the statistical approach does not allow to enforce *k*-anonymity. If sensing devices are able to communicate with each other, they can use secret sharing to cryptographically enforce *k*-anonymity of their readings [155]. However, this potentially opens another attack vector, namely for malicious users to de-anonymize benign users.

In the case of location information, *k*-anonymity can be a misleading metric. For example, when the target area is small or not diverse enough (e.g., it contains only a single point of interest), a reading can be privacy-critical if an attacker can find out a certain individual is among the *k* users [235]. To alleviate this, *l*-diversity [128] can make sure the area contains at least *l* points of interest, and hierarchical map quantization can ensure a consistent minimum size of cloaking regions [209]. Privacy guarantees are possible with differential privacy, for example by applying planar Laplace noise to obfuscate locations [135], or by adjusting the noise distribution to the point-of-interest density in an area [213].

Separation of knowledge: Splitting knowledge between different entities can reduce the risk of privacy violations. In order to access sensitive user information, these entities would then have to collude. For example, in the participatory sensing architecture presented in [40], Kapadia *et al.* split the entities that query and receive reports from the users. They also suggest the use of Direct Anonymous Attestation (DAA) to allow the server to authenticate the participants in a privacy-preserving manner (see Section III-B).

State of the Art Examples: Glasgow's (Scotland) operations center combines CCTV footage from across the city with automated video analysis to support traffic management and policing [32]. Intelligent street lights sense the presence of pedestrians or cyclists and adapt their lighting level accordingly. The street lights also include sensors to measure air pollution and noise levels, which feed back into the operations center [11]. The city's privacy policy indicates that the city relies on policies and contracts with third parties to ensure compliance with U.K. data protection law. Technical privacy protection is not mentioned.

Rio de Janeiro's center of operations integrates more than 30 departments, including emergency response, police, fire, and health with the intention of improving the response to natural disasters [10]. The center relies on location tracking of emergency vehicles, CCTV, and a joint situation room for all departments [29]. It is not clear whether this system processes data about individuals, and, if so, how it handles privacy.

Eindhoven (The Netherlands) used several sensing-based projects in a popular nightlife area, the Stratumseind [68]. Audio sensors are used to detect the level and direction of noise. To protect privacy, these sensors do not record or transmit raw sound data. Cameras are used to count the number of people on the street, and instead of saving video or image

data, the cameras detect people, count them, and immediately discard the raw video data. In partnership with Vodafone, Eindhoven uses mobile phone location data to count people and determine where they come from. To protect privacy, this data is aggregated to municipality level and only reported when more than 15 phones from the same municipality are present. Eindhoven also uses smart lights to influence ambience in the street. For example, if noise level and people counts indicate possible violence in the street, the light color and intensity can be regulated to de-escalate the situation [236]. None of the projects in Stratumseind store personal data, while fully achieving the original goal.

E. Wearable Devices

The main privacy threats for wearable devices come from wireless eavesdropping, protocol design and software flaws, and side channel attacks [75]. We note that protocol design flaws include both security issues in protocol stacks [237] as well as conceptual privacy issues, e.g., unnecessarily revealing sensitive data to medical service providers. Sensor data can be used to re-identify individuals and a wide range of their behaviors and psychological states, for example using electrocardiograms (ECG) and respiration sensors [206]. Privacy protection is thus needed at all points that handle personal sensor data, i.e., the wearable device itself, mobile devices that help transmit sensor data [64], the communication channel (see Section IV-A), and third party servers (see Section IV-I). If incorporated as part of a participatory sensor network, then all the privacy challenges of these networks (location tracking, disclosure of sensitive information) also apply to wearable devices (see Section IV-D).

Privacy for Wearables: To protect privacy, wearable devices can store the minimal amount of data necessary for their purpose. In addition, utility-neutral aggregation is often possible by adjusting the degree of time and location granularity [205]. For example, instead of a precise timestamp the wearable could store only the duration of an event. This has been shown to decrease privacy concerns [206].

Another privacy protection mechanism is to allow wearables to operate offline by processing data locally instead of uploading it to a service provider. If online operation is necessary, pre-processing on the device can extract the relevant features and discard the raw data stream. For example, a wearable device that uses audio streams to detect coughing needs to transmit this data to a physician for analysis. However, instead of streaming raw audio data, it is possible to extract invertible features from the audio stream which allows to reconstruct the cough sounds while making speech unintelligible [78].

Finally, wearables that do need to make use of a service provider can use homomorphic encryption (see Section III-B) to ensure that the provider can store and process data without being able to read it. For example, a wearable app for diabetics can locally encrypt blood glucose and glycated hemoglobin values, the cloud provider can process the encrypted data, e.g., by comparing to thresholds or computing averages, and a caregiver can decrypt and act on the processed values [99]. This solution has been implemented on a consumer-grade smart watch and is thus computationally feasible today.

Privacy for Body Area Networks: The resource constraints of body sensors pose a challenge for privacy protection in wireless body area networks [238]. To avoid eavesdropping, the communication from and between the sensors needs to be secured. Furthermore, body area networks can be susceptible to many active attacks already known in the context of conventional and ad-hoc networks, e.g., routing or man-in-the-middle attacks [239].

Additionally, sensitive data stored on the devices itself constitutes a privacy risk, because even if encrypted, the encryption key is often stored alongside [214]. Possible solutions include secure distributed data storage based on secret sharing [154] combined with fine-grained distributed role-based access control [215].

State of the Art Examples: Oulu (Finland) prototyped a city-wide running application that could track citizens' runs using the city's WiFi infrastructure [77]. The application allowed users to view statistics of their runs and find running buddies. Privacy was addressed by automatically stopping to track users after their run, however, other privacy technologies were not deployed.

Medical wearables, such as implantable medical devices and body area networks, collect more sensitive data and thus pose complex privacy challenges [75]. In many countries, medical regulations have strict requirements for the processing and storage of medical data (e.g., HIPAA in the U.S.) [74]. Fitness wearables, however, are not restricted by medical regulations, which means that companies can design their own privacy policies. Paul and Irvine [74] found that only two of the four reviewed providers of wearable devices assure that they do not make commercial use of user-generated data, while one asserts ownership of the data, and another reserves the right to commercially exploit the data.

F. Internet of Things

The Internet of Things (IoT) enhances existing appliances with sensing and communication capabilities to collect data and enable applications such as smart homes or smart buildings. This allows service providers and involved parties to learn sensitive information about the people living in the monitored space. For example, the contents of the smart fridge allow to draw conclusions about a person's nutrition and health [48] and smart meter readings can disclose exactly when and how an appliance in a household was used, or even which TV program was watched [80].

The large amounts of data shared between devices and potentially collected by the provider requires strong transport and storage security concepts. The variety of different devices also demands solutions that ensure that one compromised device does not lead to the compromise of the entire system (see [240] for a good review on the security challenges of the IoT).

Many of the privacy mechanisms for sensor networks can also be applied to the IoT (see Section IV-D). The manufacturers of smart appliances often offer cloud services as front-ends

for remote control. In this case, the privacy considerations for cloud computing (see Section IV-I) apply.

Data Minimization: Transferring data to manufacturers (or service providers) makes it difficult for users to control what data is being transferred and how it is used. This can be countered by performing operations locally on the IoT device. Cryptography can support device-local operations even if the provider has to be assured of their correctness. For example, time-of-use billing on smart meters can be realized with zero-knowledge proofs [47], [149] (see also Section III-B).

Anonymization and Aggregation: In smart grids, many grid management functions can be performed on aggregated data of entire neighborhoods instead of single households without a loss of utility [241]. This aggregation can be performed privately by a trusted third party [242], or even by an untrusted aggregator using homomorphic encryption [79], [217], secret sharing or bilinear maps [153].

IoT devices often leak sensitive data already during service discovery, for example the owner's name and the type of service. Private service discovery allows devices to only advertise their services to authorized clients, while clients can reveal their identity only after they have verified that they are communicating with the correct service [137]. Service announcements are encrypted under the authorization policy using identity-based encryption (see Section III-B) so that only authorized clients can decrypt the announcements. Private mutual authentication can be achieved in the same way.

Obfuscation: Obfuscation of energy measurements can be achieved by modifying the load signatures with a rechargeable battery [243], or by applying differential privacy [134]. IoT data streams can also be k-anonymized by dynamically clustering data and only releasing clusters with at least k members [210].

State of the Art Examples: Aspern, a suburb of Vienna (Austria), aims to integrate smart buildings, smart metering, and smart grids to optimize grid operation and energy consumption. To achieve this, they embed sensors into the electricity grid (e.g., power generation, voltage) and buildings (e.g., power consumption, ventilation, heating, water), and use data analytics to drive applications like grid anomaly detection and identification of building energy patterns. Aspern also aims to provide an open data platform that enables new business opportunities based on data collected in the city [12]. The Aspern project explores the use of privacy technologies in research, but relies mainly on user consent in the current realization of the project. Aspern recognizes that privacy policies do not inform citizens well enough about the capabilities of smart city applications. Therefore, the suburb additionally hosts information events and utilizes Internet forums to inform and engage with citizens.

The city of Zwolle (The Netherlands) operates a similar smart grid/smart building project. Following a privacy engineering process [101], Zwolle implements data minimization by performing most computations locally in-home, uses data aggregated to residential area level, and separates knowledge between the energy supplier (billing data) and the operator of the distribution network (no link to personal data) [15].

The city of Bristol (U.K.) has enhanced 1,500 of its street lamps with heat, sound, light, and air quality sensors. In addition, the street lamps form a wireless mesh network that is connected to the city's fiber network [11]. The network and sensors are not yet available for public use, but only as an experimentation testbed for researchers and developers of proprietary applications. Even though the network and sensors are operating in the city's public space, there is no information regarding privacy, especially regarding what data might be collected and stored from passersby.

G. Autonomous Systems

Autonomous systems, such as robots and drones, are still in the early phases of adoption. To enable autonomous operation, these systems rely on various sensors, which can give manufacturers and operators of autonomous systems access to sensitive data about the individuals the robot or drone comes into contact with. For example, shipping companies are testing autonomous drones for faster delivery. Domestic robots for kitchen or cleaning tasks are already available on the market and prototypes of robots for elderly care were presented not only to engage in conversation [244] but also carry out nursing care tasks [245]. Other robots include teaching robots [246] which, when exploited, could generate accurate profiles of citizens from an early age.

Data minimization: Outdoor autonomous systems usually come with a variety of sensors to support maneuvering and other tasks, and therefore the privacy challenges are similar to those of sensor networks (see Section IV-D). The sensors of a robot can gather much more data than needed for operation and this collateral data could be exploited to learn about citizens. For example, a robot emptying waste containers could analyze the contents to learn information about the owner, and a delivery drone using cameras for navigation could transmit photographs of private property.

For indoor robots, the privacy challenges are similar to the Internet of Things (see Section IV-F). These systems operate in the most private place of citizens, that is, their home and therefore have access to sensitive information. With more and more human-like robots, people could also voluntarily disclose private information as they might start perceiving the system as a companion.

Privacy for mobility services: Autonomous vehicles are envisioned to make public transport more efficient. The privacy implications are similar to today's account-bound taxi services, where each trip is automatically stored by the provider. With a high availability of autonomous taxis, people may choose to give up owning a private vehicle and thus the taxi provider could gain a much more complete view of people's location tracks. Anonymous usage of these services, i.e., anonymous payment and authentication, can be realized with anonymous or pseudonymous credentials (see Section III-B).

State of the Art Examples: Several locations in California (USA) have deployed the crime-fighting robot Knightscope K5, including shopping malls, the Microsoft campus [247], and the Bakersfield Memorial Hospital [248]. The robot can be

rented via a machine-as-a-service model which includes hardware, software, and data storage. Using a wide range of sensors that include a 360° camera, infrared cameras, audio sensors, thermal sensors, license plate recognition, ranging (LIDAR), GPS, and proximity sensors, the robot autonomously conducts surveillance in an area and sends the data back to an operations center, gathering 90TB of data per year. While Knightscope designed the robot to encrypt data communications using WPA2 and SSL, the company claims that there is no expectation of privacy in public places and thus the robot does not implement any privacy features that would protect the privacy of individuals in a meaningful way.

In Waseda (Japan), the humanoid robot Pepper is used to help high school students study English [249], [250]. Despite its humanoid appearance, Pepper is equipped with a wide range of sensors and an Internet connection. Pepper uses online services for speech recognition and a cloud solution allows to manage and remotely monitor the robot. Any interactions with school children are thus at risk of being subject to remote surveillance, which would allow profiling of children. Despite this risk, information about privacy and privacy protections are not available, neither from the school nor from the manufacturer.

H. Intelligent Vehicles

For traffic safety applications, vehicles periodically broadcast their status (including their identity, position, heading, speed, state of the turn signals, etc.) with a frequency of 1 to 10 Hz. Other vehicles in the vicinity can then receive and react to these broadcasts, e.g., by braking automatically or warning the driver. Because these broadcasts are unencrypted, everyone in transmission range can link vehicles to locations and track their paths [88]. The same broadcasts can also be received by infrastructure nodes such as traffic lights or traffic signs and used for traffic efficiency applications.

Pseudonymity: The privacy protection suggested by the upcoming IEEE and ETSI standards relies on vehicles using a pool of short-term pseudonyms for ad-hoc communication (see Section III-B). The level of privacy protection achievable with this system depends on how vehicles change their pseudonyms [160], however, concrete pseudonym changing strategies are still missing in the standards [88]. Furthermore, pseudonyms can be de-anonymized using meta data (e.g., home and work addresses [251]), and the changing of pseudonyms does not prevent tracking if the attacker is within transmission range [221]. This can be addressed by making all vehicles change their short-term identifiers simultaneously [220], which maximizes privacy for vehicles not under attacker surveillance. To avoid confusing nearby vehicles and thereby reducing safety, pseudonym changes can be announced locally [221].

Knowledge Separation: The entity running the Certificate Authority (CA) knows the mapping from short-term to long-term identifier, which allows repurposing of transmitted messages to install automated traffic surveillance [88]. While there are mechanisms that eliminate this mapping, e.g., blind signatures [157] or pseudonym exchanging [220], they interfere with the requirements for accountability and law enforcement and are thus unlikely to be deployed [88]. In addition to policies regulating when the CA is allowed to de-anonymize pseudonyms, knowledge separation requires multiple institutions to collude to achieve de-anonymization and thus prevents misuse of the CA's capabilities [207].

Backwards Privacy: To exclude a vehicle from the network, all its identifiers need to be revoked. Publishing a list with all pseudonyms would disclose the privacy of the vehicle in retrospect [89]. Therefore, certificate revocation schemes that are backwards-privacy preserving have been proposed to only revoke future short-term identities of a car [89], [222].

Service and Device Integration: The integration of intelligent vehicles into convenience applications, such as wireless payments at gas stations or toll gates, can increase the number of data holders and further complicate privacy issues. Toll payments based on actual road usage can be performed in a privacy-preserving way using local price calculation and cryptographic commitments [150].

Already today, car manufacturers are collecting large amounts of potentially sensitive driver information [252]. This information may find its way to third-party apps through in-vehicle app stores, either built-in or plugged into the vehicle's on-board diagnostic (OBD) port [253], and thus exacerbate privacy issues known from smartphones [6]. Since there is large interest in collecting user information – up to the point where "there [could] come a time when more money is made from the sale of private data as opposed to the initial car purchase" [253], it is also the responsibility of the legislative authorities to ensure against the risks of privacy violation.

State of the Art Examples: From 2018 on, all new vehicles within the European Union are mandated to be equipped with the cellular service based eCall emergency system [254]. The eCall regulations mandate that vehicles are not traceable during normal vehicle operation. To achieve this, the system only connects to the mobile phone system when a serious accident happens and stores previous vehicle locations only to determine the direction of travel at the time of an accident [86]. However, the eCall regulations only protect the basic eCall system, but do not cover additional services. For example, insurance companies may access the data to determine insurance premiums, and law enforcement may remotely track individuals [255].

Drivers are often insufficiently informed about which data is collected by their vehicle, and by whom it is accessed. A recent example concerned a driver using BMW's shared car service DriveNow. After running over a cyclist, the driver was convicted because the car had recorded information about the car's location and speed – despite DriveNow's claims that it doesn't store such data [87]. While assisting the conviction was certainly a noble cause, the system in general is privacy-invasive and open to misuse, especially when customers are misled into believing that the car does not store data.

In the context of cooperative transportation systems, Japan has reserved the 760 MHz frequency for vehicular communications [256]. Several of Toyota's production cars ship with a cruise control system that uses vehicle-to-vehicle communication to maintain inter-vehicle distances, and with a

collision caution system that communicates with road-side units to avoid turning collisions at intersections. In collaboration with the Japanese government, Toyota has deployed 47 road-side units in Tokyo, Nagoya City, and Toyota City [257]. Information about the privacy implications of Toyota's technology is not readily available.

In the last years, autonomous driving has received attention from car manufacturers (e.g., BMW, AUDI, Toyota) and IT companies (Google, Apple) alike [258], and semi-autonomous vehicles such as the Tesla Model S can already be bought today. In 2016, autonomous taxis have been first introduced in Singapore and are planned to be deployed in the thousands [258]; information on data protection and privacy was not available.

I. Cloud Computing

Cloud providers are used as part of public-private partnerships to outsource storage and/or processing of arbitrary smart city data and services. This makes it necessary to consider privacy in the context of cloud computing in addition to the considerations for the underlying data or service. Securing data in transit (see Section IV-A) is a necessary but not sufficient measure. Privacy also needs to be protected while data is being stored and/or processed at the cloud provider [259].

Privacy for Outsourced Storage: A straightforward solution to protect outsourced storage is to only store encrypted data. However, even though the storage provider cannot see the contents of the encrypted data, access patterns may leak sensitive information. Private information retrieval protocols allow to hide the access patterns to remote files [167] or queries to remote databases [166]. Attribute-based encryption (see Section III-B) is a one-to-many encryption method that can be used, for example, to share personal health records. By encrypting data not with a single key, but a set of attributes, patients can exert fine-grained control over which groups of people can access which parts of the health record [139], [140].

Privacy for Outsourced Processing: When users have to authenticate at the cloud provider before data processing can take place, attribute-based credentials allow authentication without revealing the user's identity, making sure that the cloud provider cannot track the actions of individual users [19]. Secure multi-party computations are used when multiple parties are interested in the results of a joint computation, but do not want to reveal their private inputs [223]. Privacy-preserving data mining allows to learn useful information from distributed datasets, which can either be distributed vertically (entities hold different attributes) or horizontally (entities hold data about different users) [224]. Homomorphic encryption enables computations over encrypted data [143].

State of the Art Examples: Copenhagen's (Denmark) smart city project, Copenhagen Connecting, operates a city-wide mesh of WiFi hotspots that can locate and track mobile phones to improve traffic flow and safety [22]. This project uses cloud services provided by a third-party company to store and process data, and to provide a Web frontend. The company operating this service claims that the information is aggregated and anonymized before being transmitted [91], but does not further substantiate the claim.

V. Discussion

Our survey shows the complexity of privacy in the smart city including a large number of challenges and possible solutions. The sheer magnitude of systems and technologies make the creation of a privacy-friendly smart city a gargantuan or even seemingly impossible task. However, we believe that there are guidelines and research directions which can be followed to significantly increase the level of privacy in future smart cities. This does not necessarily mean creating new privacy-enhancing technologies but rather applying existing ones on a large scale, effectively taking a more holistic approach. In this section, we discuss challenges and point to promising research directions that have not yet been widely considered in the context of smart cities.

Optimizing the Privacy Design Process: When designing a new smart city application, a standardized design process could greatly assist in ensuring appropriate privacy protection. This design process needs to integrate existing methods, e.g., privacy requirements engineering and privacy testing (see Section III-A) into a holistic process. In the software engineering world, many design processes have been proposed, however, it is unclear how privacy design should be integrated into these. There are some proposals, e.g., the MITRE V-model [260] or a method to incorporate privacy by design in agile environments [261], however, more research is needed to find out which is the best design process in which setting. Especially with regard to the high level of interconnectivity and complexity in smart cities, safeguarding single applications with a privacy design process might not be sufficient. Instead there may be a need for a general design process for smart cities that guides how to make a city smart with the privacy requirements of its citizens in mind.

Joint or Composable Privacy Technologies: It is evident from our discussion in Section IV that due to the diversity of smart city applications, different privacy technologies need to be combined to achieve an acceptable level of privacy. Indeed, smart cities combine so many technological components that it is not enough to simply apply privacy technologies to each component. Instead, we argue that the interactions between technologies and data have to be considered to design joint privacy technologies [205]. This is especially important because many smart cities start with isolated solutions that get integrated gradually. One method to facilitate joint privacy protection is to focus on the interfaces between different systems, on their level of interconnectivity and most importantly on the data exchanged. For example, different components in a sensing architecture could all (sequentially or in parallel) deploy independent differential privacy mechanisms before transmitting or publishing data [127].

Privacy Architecture Patterns: Architecture patterns describe a system's components, their responsibilities, and the relationships between them. (Design patterns are used to refine the components and their relationships.) The lack of

existing privacy architecture patterns leads to the development of custom architectures.

As described in Section III-A, we have found two groups of privacy architectures in the literature. The first group contains variations of a simple centralized architecture that does not take into account the diversity of attackers and smart city applications. Examples include proposals to safeguard all data in a central repository either controlled by the government [262] or a cloud provider [6], potentially mediated by a broker [12]. The second group contains specialized architectures that are tailored to specific application areas within the smart city, for example smart health care [122].

The cost of making smart cities privacy-friendly could be reduced if developers could apply an existing privacy architecture, that is, they have guidelines, patterns, and tools available to layout their system. This would include how different systems should exchange data, where data is collected, and what data is stored. Ideally, privacy architectures would also encompass a modeling language to describe, layout, and share different architectural approaches. This language should include semantics to assign privacy risk levels to components and data streams, and also describe properties of interaction between components (e.g., encrypted or plain text). This helps understand information flow and identify possible risks and points of attack, thus supporting the design of privacy-preserving system layouts.

Incentives and Enforcement: Both joint privacy mechanisms and privacy architectures aim to integrate isolated privacy protection mechanisms into more general or even holistic solutions. In smart cities, this integration is complicated not only by a large number of subsystems, but also by a large number of stakeholders. To implement joint privacy mechanisms in a coherent privacy architecture, various stakeholders will have to work together on an operational level. However, this collaboration can entail severe privacy risks because it may enable stakeholders to combine data from several sources. To mitigate these risks and realize the full potential of privacy-friendly smart cities, cities need to set incentives that encourage privacy-friendly collaboration and introduce ways to enforce privacy-friendliness.

Game theory has already been applied successfully to privacy problems, for example in vehicular networks and anonymous communication, and has also been used to identify which incentives can encourage desired behaviors (see [263] and the references therein). We believe that game theoretic studies will be an important tool to understand how privacy-friendly behaviors can be encouraged in a time when privacy violation constitutes a business case [5].

Blockchains are a promising technology that may be able to enforce privacy properties. Blockchains are distributed immutable ledgers that record and store transactions which can be publicly verified. New transactions are bundled in blocks and appended to the ledger (or *mined*) by solving a cryptographic puzzle. Each new block is linked to its predecessor (hence the name block chain). In blockchains, users enjoy pseudonymity because they are only identified by their public keys, and there is no need for a trusted third party because a distributed consensus is achieved through the mining of blocks. Originally introduced for financial transactions in Bitcoin [264], researchers have started to apply blockchains to non-financial problems. For example, there exist proposals to use blockchains to improve security and privacy in the Internet of Things [265] (see Section IV-F), and to use blockchains as "decentralized personal data management systems" that allow users to own and control their data [266]. We believe that more research is needed to explore whether and how blockchains can be used for privacy enforcement in smart city environments.

User-centric Privacy: It seems only logical to involve the users more in the technology that is aimed to improve their quality of life, but can also affect their privacy. Unfortunately, the large number of services and citizens makes it infeasible to manually consider user-centric privacy preferences – for both the service provider and the citizen. Ideally, citizens would be able to specify their privacy preferences and smart city services would automatically adapt to the user preferences or warn the user, if not possible. This would enable users to opt-out of data storage, or even an entire service. This may require new kinds of user interfaces that allow citizens to give meaningful consent (see Section III-A).

Where possible, service quality should not depend on user privacy settings to avoid punishing more private users. Many solutions we have discussed in Section IV protect privacy while fully preserving utility [96], for example aggregation in smart metering using homomorphic encryption or secret sharing [79], [153], [217], or device-local data processing for medical [78] or people-counting applications [68].

Trade-off between Privacy and Utility: Privacy-enhancing technologies are often not adopted because of a fear that they will degrade data quality to a point where the quality of the provided service is affected. Even though we have discussed several utility-neutral privacy mechanisms, we believe that more research is needed to show how privacy-enhancing technologies affect the utility of smart city services.

This problem needs to be tackled from both sides: First, operators, standards, and service providers should define more specifically what data (and with which accuracy) is required for the proper functioning of an application. Data overcollection can only be stopped if it is clear what portion of data is essential for an application, and what portion is not. For example, in the context of communicating vehicles (see Section IV-H), message formats for road hazard warnings as defined by the ETSI ITS-G5 standards include sequence numbers which are not required to warn other drivers, yet could be exploited to track vehicles [88].

Second, privacy researchers and engineers should keep the required level of utility in mind when developing privacy-enhancing technologies to increase the likelihood of adoption. To protect location privacy in vehicular ad-hoc networks, for example, several methods were proposed that heavily interfere with the main goal of improving traffic safety, even though adequate privacy protection can be achieved without affecting traffic safety [221].

Privacy Awareness: Lastly, we believe that awareness for the privacy risks that go along with the introduction of many smart city applications and technologies needs to be increased. People need to better understand that personal data has a value

attached to it and that it even can be seen as a kind of currency [267], [268]. Increasing this awareness is a challenging task, because it cannot be directly influenced by researchers but lies in the hands of the media and political powers. Unfortunately, it seems that only if there is a user-driven demand for privacy, can protection mechanisms be an integral part of the development and deployment process. Smart cities need to embrace privacy-by-design principles from the get go, because retrofitting privacy is bound to fail.

VI. Conclusion

Smart cities are complex. Various concepts, applications and technologies interact to encompass every aspect of the digital citizen's life. Understanding this privacy-challenging environment is the basic requirement for the development of effective protection mechanisms. We analyzed smart cities around the world and found that, with few exceptions, privacy protection or even information on privacy policies is still scarce. This survey contributes to improving this situation.

To break down the complexity of the smart city, we introduced taxonomies for application areas, enabling technologies, potential attackers, data sources for attacks, and different types of citizens' privacy. These taxonomies allowed us to present a holistic analysis of privacy threats and possible solutions. We found many utility-neutral techniques, indicating that the privacy-utility tradeoff may be less severe than usually thought. We also observed that privacy solutions for different technologies are often similar, indicating the possibility of generic privacy patterns. These patterns along with a well-defined privacy architecture can contribute to the integration of the many tailored privacy solutions found in the literature.

In summary, we hope that our systematic review of privacy in smart cities will support comprehensive privacy solutions for smart cities.

Acknowledgment

The authors would like to thank the anonymous reviewers for their insightful and in-depth comments which have helped to greatly improve the paper.

References

[1] European Union. (2016). *Market Place of the European Innovation Partnership on Smart Cities and Communities*. Accessed: Aug. 30, 2017. [Online]. Available: https://eu-smartcities.eu/

[2] A. Caragliu, C. Del Bo, and P. Nijkamp, "Smart cities in Europe," *J. Urban Technol.*, vol. 18, no. 2, pp. 65–82, Aug. 2011.

[3] N. Komninos, *The Age of Intelligent Cities: Smart Environments and Innovation-for-All Strategies*, vol. 78. London, U.K.: Routledge, Aug. 2014.

[4] K. Su, J. Li, and H. Fu, "Smart city and the applications," in *Proc. IEEE Int. Conf. Electron. Commun. Control (ICECC)*, Ningbo, China, Sep. 2011, pp. 1028–1031.

[5] P. M. Schwartz, "Property, privacy, and personal data," *Harvard Law Rev.*, vol. 117, no. 7, pp. 2056–2128, May 2004.

[6] Y. Li, W. Dai, Z. Ming, and M. Qiu, "Privacy protection for preventing data over-collection in smart city," *IEEE Trans. Comput.*, vol. 65, no. 5, pp. 1339–1350, May 2016.

[7] B. Cohen. (Nov. 2014). *The Smartest Cities in the World 2015: Methodology*. Accessed: Aug. 30, 2017. [Online]. Available: https://www.fastcompany.com/3038818/the-smartest-cities-in-the-world-2015-methodology

[8] Juniper Research. (Feb. 2015). *Barcelona Named 'Global Smart City—2015'*. Accessed: Aug. 30, 2017. [Online]. Available: http://www.juniperresearch.com/press/press-releases/barcelona-named-global-smart-city-2015

[9] P. Berrone and J. E. Ricart, "IESE cities in motion index 2016," IESE Bus. School, Barcelona, Spain, Tech. Rep. ST-396-E, May 2016.

[10] V. Buscher and L. Doody, "Global innovators: International case studies on smart cities," Dept. Bus., Innov. Skills, Ove Arup & Partners Ltd., London, U.K., BIS Tech. Rep. 135, Oct. 2013.

[11] E. Woods, D. Alexander, R. R. Labastida, and R. Watson, "U.K. smart cities index—Assessment of strategy and execution of the U.K.'s leading smart cities," Huawei, Shenzhen, China, Tech. Rep., May 2016. [Online]. Available: http://www-file.huawei.com/~/media/CORPORATE/PDF/News/Huawei_Smart_Cities_Report_FINAL.pdf?la=en

[12] D. Dhungana, G. Engelbrecht, J. X. Parreira, A. Schuster, and D. Valerio, "Aspern smart ICT: Data analytics and privacy challenges in a smart city," in *Proc. IEEE 2nd World Forum Internet Things (WF IoT)*, Milan, Italy, Dec. 2015, pp. 447–452.

[13] A. Ståhlbröst, A. Padyab, A. Sällström, and D. Hollosi, "Design of smart city systems from a privacy perspective," *Int. J. WWW/Internet*, vol. 13, no. 1, pp. 1–16, 2015.

[14] L. Cilliers and S. Flowerday, "Information privacy concerns in a participatory crowdsourcing smart city project," *J. Internet Technol. Secured Trans.*, vol. 3, nos. 3–4, pp. 280–287, Sep. 2014.

[15] C. M. Portela *et al.*, "A flexible, privacy enhanced and secured ICT architecture for a smart grid project with active consumers in the city of Zwolle—NL," in *Proc. 22nd Int. Conf. Electricity Distrib. (CIRED)*, Stockholm, Sweden, Jun. 2013, pp. 1–4.

[16] D. Geronimo, A. M. Lopez, A. D. Sappa, and T. Graf, "Survey of pedestrian detection for advanced driver assistance systems," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 32, no. 7, pp. 1239–1258, Jul. 2010.

[17] H. Hartenstein and K. P. Laberteaux, "A tutorial survey on vehicular ad hoc networks," *IEEE Commun. Mag.*, vol. 46, no. 6, pp. 164–171, Jun. 2008.

[18] R. Bodenheimer, A. Brauer, D. Eckhoff, and R. German, "Enabling GLOSA for adaptive traffic lights," in *Proc. 6th IEEE Veh. Netw. Conf. (VNC)*, Paderborn, Germany, Dec. 2014, pp. 167–174.

[19] A. Avgerou, P. E. Nastou, D. Nastouli, P. M. Pardalos, and Y. C. Stamatiou, "On the deployment of citizens' privacy preserving collective intelligent eBusiness models in smart cities," *Int. J. Security Appl.*, vol. 10, no. 2, pp. 171–184, Feb. 2016.

[20] D. Belanche-Gracia, L. V. Casaló-Ariño, and A. Pérez-Rueda, "Determinants of multi-service smartcard success for smart cities development: A study based on citizens' privacy and security perceptions," *Govern. Inf. Quart.*, vol. 32, no. 2, pp. 154–163, Apr. 2015.

[21] A. W. Burange and H. D. Misalkar, "Review of Internet of Things in development of smart cities with data management & privacy," in *Proc. Int. Conf. Adv. Comput. Eng. Appl. (ICACEA)*, Ghaziabad, India, Mar. 2015, pp. 189–195.

[22] L. H. Carlsen, "The location of privacy—A case study of Copenhagen connecting's smart city," M.S. thesis, Dept. Commun. Bus. Inf. Technol., Roskilde Univ., Roskilde, Denmark, Aug. 2014.

[23] A. Martínez-Ballesté, P. A. Pérez-Martínez, and A. Solanas, "The pursuit of citizens' privacy: A privacy-aware smart city is possible," *IEEE Commun. Mag.*, vol. 51, no. 6, pp. 136–141, Jun. 2013.

[24] P. Asmus, "Microgrids, virtual power plants and our distributed energy future," *Electricity J.*, vol. 23, no. 10, pp. 72–82, Dec. 2010.

[25] B. Dunn, H. Kamath, and J.-M. Tarascon, "Electrical energy storage for the grid: A battery of choices," *Science*, vol. 334, no. 6058, pp. 928–935, Nov. 2011.

[26] A. Ståhlbröst, A. Sällström, and D. Hollosi, "Audio monitoring in smart cities—An information privacy perspective," in *Proc. 12th Int. Conf. e-Soc.*, Madrid, Spain, Feb. 2014, pp. 35–44.

[27] A. Bartoli *et al.*, "Security and privacy in your smart city," in *Proc. Barcelona Smart Cities Congr.*, Barcelona, Spain, Dec. 2011, pp. 1–6.

[28] C. Gomez and J. Paradells, "Wireless home automation networks: A survey of architectures and technologies," *IEEE Commun. Mag.*, vol. 48, no. 6, pp. 92–101, Jun. 2010.

[29] V. Durani. (Nov. 2011). *City of Rio de Janeiro and IBM Collaborate to Advance Emergency Response System*. Accessed: Aug. 30, 2017. [Online]. Available: http://www-03.ibm.com/press/us/en/pressrelease/35945.wss

[30] F. Wenzel, M. C. Oncescu, M. Baur, F. Fiedrich, and C. Ionescu, "An early warning system for Bucharest," *Seismol. Res. Lett.*, vol. 70, no. 2, pp. 161–169, Mar. 1999.

[31] G. Baldini, I. Kounelis, I. N. Fovino, and R. Neisse, "A framework for privacy protection and usage control of personal data in a smart city scenario," in *Critical Information Infrastructures Security* (LNCS 8328). Cham, Switzerland: Springer, Sep. 2013, pp. 212–217.

[32] L. Edwards, "Privacy, security and data protection in smart cities: A critical EU law perspective," *Eur. Data Protect. Law Rev.*, vol. 2, no. 1, pp. 28–58, 2016.

[33] Stockholm City Executive Office. (2010). *Living in Stockholm Should Be e-asy*. Accessed: Aug. 30, 2017. [Online]. Available: http://international.stockholm.se/globalassets/ovriga-bilder-och-filer/e-tjanster_broschyr-16-sid_4.pdf

[34] A. S. Elmaghraby and M. M. Losavio, "Cyber security challenges in smart cities: Safety, security and privacy," *J. Adv. Res.*, vol. 5, no. 4, pp. 491–497, Jul. 2014.

[35] A. Solanas *et al.*, "Smart health: A context-aware health paradigm within smart cities," *IEEE Commun. Mag.*, vol. 52, no. 8, pp. 74–81, Aug. 2014.

[36] M. Duggan. (May 2017). *Technology for Autism Now*. Accessed: Aug. 30, 2017. [Online]. Available: https://web.archive.org/web/20160505043851/http://newurbanmechanics.org/project/technology-for-autism-now/

[37] A. Cimmino *et al.*, "The role of small cell technology in future smart city applications," *Trans. Emerg. Telecommun. Technol. Special Issue Smart Cities*, vol. 25, no. 1, pp. 11–20, Jan. 2014.

[38] R. C.-W. Phan and L. A. Mohammed, "On the security & design of MyKad," in *Proc. 9th Asia–Pac. Conf. Commun. (APCC)*, Penang, Malaysia, Sep. 2003, pp. 721–724.

[39] *Identification Cards—Contactless Integrated Circuit Cards—Proximity Cards*, ISO/IEC Standard 14443-2016, Jun. 2016.

[40] A. Kapadia, N. Triandopoulos, C. Cornelius, D. Peebles, and D. Kotz, "AnonySense: Opportunistic and privacy-preserving context collection," in *Pervasive Computing* (LNCS 5013). Heidelberg, Germany: Springer, May 2008, pp. 280–297.

[41] T. Martin, E. Jovanov, and D. Raskovic, "Issues in wearable computing for medical monitoring applications: A case study of a wearable ECG monitoring device," in *Proc. 4th IEEE Int. Symp. Wearable Comput.*, Atlanta, GA, USA, Oct. 2000, pp. 43–49.

[42] *FCC Dedicates Spectrum Enabling Medical Body Area Networks to Transform Patient Care, Lower Health Care Costs, and Spur Wireless Medical Innovation*, Federal Commun. Commission, Washington, DC, USA, May 2012, accessed: Aug. 30, 2017. [Online]. Available: https://www.fcc.gov/document/fcc-dedicates-spectrum-enabling-medical-body-area-networks

[43] H. Yao, C. Marcheselli, A. Afanasiev, I. Lähdesmäki, and B. A. Parviz, "A soft hydrogel contact lens with an encapsulated sensor for tear glucose monitoring," in *Proc. IEEE 25th Int. Conf. Micro Electro Mech. Syst. (MEMS)*, Paris, France, Feb. 2012, pp. 769–772.

[44] S. Coyle *et al.*, "Smart nanotextiles: A review of materials and applications," *MRS Bull.*, vol. 32, no. 5, pp. 434–442, May 2007.

[45] ITU Telecommunication Standardization Sector, "Overview of the Internet of Things," Int. Telecommun. Union, Geneva, Switzerland, Tech. Rep. ITU-T Y.2060, Jun. 2012.

[46] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A survey on enabling technologies, protocols, and applications," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 2347–2376, 4th Quart., 2015.

[47] A. Rial and G. Danezis, "Privacy-preserving smart metering," in *Proc. 18th ACM Conf. Comput. Commun. Security (CCS) 10th Workshop Privacy Electron. Soc. (WPES)*, Chicago, IL, USA, Oct. 2011, pp. 49–60.

[48] S. Luo, J. Jin, and J. Li, "A smart fridge with an ability to enhance health and enable better nutrition," *Int. J. Multimedia Ubiquitous Eng.*, vol. 4, no. 2, pp. 66–80, Apr. 2009.

[49] H.-C. Jo, S. Kim, and S.-K. Joo, "Smart heating and air conditioning scheduling method incorporating customer convenience for home energy management system," *IEEE Trans. Consum. Electron.*, vol. 59, no. 2, pp. 316–322, May 2013.

[50] D. J. Fagnant and K. M. Kockelman, "The travel and environmental implications of shared autonomous vehicles, using agent-based model scenarios," *Transp. Res. C Emerg. Technol.*, vol. 40, pp. 1–13, Mar. 2014.

[51] C. Bolkcom and J. Gertler, "Homeland security: Unmanned aerial vehicles and border surveillance," Congressional Res. Service, Washington, DC, USA, Tech. Rep. 7-5700 RS21698, Jul. 2010.

[52] D. Eckhoff, N. Sofra, and R. German, "A performance study of cooperative awareness in ETSI ITS G5 and IEEE WAVE," in *Proc. 10th IEEE Conf. Wireless Demand Netw. Syst. Services (WONS)*, Banff, AB, Canada, Mar. 2013, pp. 196–200.

[53] J. Zachariah, J. Gao, A. Kornhauser, and T. Mufti, "Uncongested mobility for all: A proposal for an area wide autonomous taxi system in New Jersey," in *Proc. 93rd Annu. Meeting Transp. Res. Board*, Washington, DC, USA, Jan. 2014, p. 14.

[54] T. Litman, "Parking management: Strategies, evaluation and planning," Victoria Transp. Policy Inst., Victoria, BC, Canada, Tech. Rep. 07-1581, Nov. 2013.

[55] H. Takabi, J. B. D. Joshi, and G.-J. Ahn, "Security and privacy challenges in cloud computing environments," *IEEE Security Privacy*, vol. 8, no. 6, pp. 24–31, Nov./Dec. 2010.

[56] S. D. Warren and L. D. Brandeis, "The right to privacy," *Harvard Law Rev.*, vol. 4, no. 5, pp. 193–220, Dec. 1890.

[57] D. J. Solove, "A taxonomy of privacy," *Univ. Pennsylvania Law Rev.*, vol. 154, no. 3, pp. 477–564, Jan. 2006.

[58] H. Nissenbaum, "Privacy as contextual integrity," *Washington Law Rev.*, vol. 79, no. 1, pp. 119–158, Feb. 2004.

[59] R. Clarke, *Introduction to Dataveillance and Information Privacy, and Definitions of Terms*, Xamax Consultancy, Chapman, ACT, Australia, Aug. 1997.

[60] A. Pfitzmann and M. Hansen. (Aug. 2010). *A Terminology for Talking About Privacy by Data Minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management v0.34*. [Online]. Available: http://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.34.pdf

[61] R. L. Finn, D. Wright, and M. Friedewald, "Seven types of privacy," in *Proc. 5th Int. Conf. Comput. Privacy Data Protect. Eur. Data Protect. Coming Age*, Brussels, Belgium, Jan. 2012, pp. 3–32.

[62] P. S. Churchland, *Brain-Wise: Studies in Neurophilosophy*. Cambridge, MA, USA: MIT Press, 2002.

[63] Hong Kong Government Digital Service. (Mar. 2017). *GovWiFi Programme Overview*. Accessed: Aug. 30, 2017. [Online]. Available: http://theme.gov.hk/en/theme/wifi/program/

[64] C. Spensky *et al.*, "SoK: Privacy on mobile devices—It's complicated," in *Proc. Privacy Enhanc. Technol. Symp.*, Darmstadt, Germany, Jul. 2016, pp. 96–116.

[65] N. Cheng, X. O. Wang, W. Cheng, P. Mohapatra, and A. Seneviratne, "Characterizing privacy leakage of public WiFi networks for users on travel," in *Proc. IEEE INFOCOM*, Turin, Italy, Apr. 2013, pp. 2769–2777.

[66] J. Ng. (Aug. 2010). *Octopus CEO Resigns Over Data Sale*. Accessed: Aug. 30, 2017. [Online]. Available: http://www.wsj.com/articles/SB10001424052748704017904575409243344854622

[67] S. M. Elaluf-Calderwood, J. Liebenau, and Patrik, *Privacy, Identity and Security Concerns: Enterprise Strategic Decision Making and Business Model Development for Mobile Payments in NFC*, Soc. Sci. Res. Netw., Brooklyn, NY, USA, Mar. 2012.

[68] I. van de Kerk, "Data use versus privacy protection in public safety in smart cities," M.S. thesis, Faculty Geosci., Utrecht Univ., Utrecht, The Netherlands, Feb. 2015.

[69] H. Rippe. (Mar. 2013). *Plan om P2000 aan banden te leggen betekent doodsteek voor 'fotocowboys'*. Accessed: Aug. 30, 2017. [Online]. Available: http://www.omroepbrabant.nl/?news/190507812/Plan+om+P2000+aan+banden+te+leggen+betekent+doodsteek+voor+fotocowboys.aspx

[70] 2CoolMonkeys. (2016). *Smart City Den Haag*. Accessed: Aug. 30, 2017. [Online]. Available: http://denhaag.smartcityapp.nl/

[71] StraatInfo.nl. (2016). *Alarmeringen*. Accessed: Aug. 30, 2017. [Online]. Available: http://almere.straatinfo.nl/alarmeringen/

[72] A. Narayanan and V. Shmatikov, "Robust de-anonymization of large sparse datasets," in *Proc. IEEE Symp. Security Privacy*, Oakland, CA, USA, May 2008, pp. 111–125.

[73] M. Gruteser and D. Grunwald, "Anonymous usage of location-based services through spatial and temporal cloaking," in *Proc. 1st ACM Int. Conf. Mobile Syst. Appl. Services (MobiSys)*, San Francisco, CA, USA, May 2003, pp. 31–42.

[74] G. Paul and J. Irvine, "Privacy implications of wearable health devices," in *Proc. 7th ACM Int. Conf. Security Inf. Netw. (SIN)*, Glasgow, U.K., Sep. 2014, pp. 117–121.

[75] M. Rushanan, A. D. Rubin, D. F. Kune, and C. M. Swanson, "SoK: Security and privacy in implantable medical devices and body area networks," in *Proc. IEEE Symp. Security Privacy*, San Jose, CA, USA, May 2014, pp. 524–539.

[76] S. Patel, H. Park, P. Bonato, L. Chan, and M. Rodgers, "A review of wearable sensors and systems with application in rehabilitation," *J. Neuroeng. Rehabil.*, vol. 9, p. 21, Apr. 2012.

[77] F. Gil-Castineira *et al.*, "Experiences inside the ubiquitous Oulu smart city," *Computer*, vol. 44, no. 6, pp. 48–55, Jun. 2011.

[78] E. C. Larson, T. Lee, S. Liu, M. Rosenfeld, and S. N. Patel, "Accurate and privacy preserving cough sensing using a low-cost microphone," in *Proc. 13th Int. Conf. Ubiquitous Comput. (UbiComp)*, Beijing, China, Sep. 2011, pp. 375–384.

[79] F. Li, B. Luo, and P. Liu, "Secure information aggregation for smart grids using homomorphic encryption," in *Proc. 1st Int. Conf. Smart Grid Commun. (SmartGridComm)*, Gaithersburg, MD, USA, Oct. 2010, pp. 327–332.

[80] U. Greveler, P. Glösekötterz, B. Justusy, and D. Loehr, "Multimedia content identification through smart meter power usage profiles," in *Proc. Int. Conf. Inf. Knowl. Eng. (IKE)*, Las Vegas, NV, USA, Jul. 2012, pp. 383–390.

[81] I. D. Manta and D. S. Olson, "Hello Barbie: First they will monitor you, then they will discriminate against you. Perfectly," *Alabama Law Rev.*, vol. 67, no. 1, pp. 135–187, Mar. 2015.

[82] T. Denning, Z. Dehlawi, and T. Kohno, "In situ with bystanders of augmented reality glasses: Perspectives on recording and privacy-mediating technologies," in *Proc. 32nd Annu. ACM Conf. Human Factors Comput. Syst. (CHI)*, Toronto, ON, Canada, Apr./May 2014, pp. 2377–2386.

[83] E. Vattapparamban, İ. Güvenç, A. İ. Yurekli, K. Akkaya, and S. Uluağaç, "Drones for smart cities: Issues in cybersecurity, privacy, and public safety," in *Proc. IEEE Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Paphos, Cyprus, Sep. 2016, pp. 216–221.

[84] T. Denning, C. Matuszek, K. Koscher, J. R. Smith, and T. Kohno, "A spotlight on security and privacy risks with future household robots: Attacks and lessons," in *Proc. 11th ACM Int. Conf. Ubiquitous Comput. (Ubicomp)*, Orlando, FL, USA, Sep. 2009, pp. 105–114.

[85] R. Calo, "Robots and Privacy," in *Robot Ethics: The Ethical and Social Implications of Robotics*. Oxford, U.K.: MIT Press, May 2010.

[86] European Commission. (Jun. 2014). *eCall—Do You Have Any Concerns for Your Privacy? You Shouldn't...* Accessed: Aug. 30, 2017. [Online]. Available: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=5963

[87] M. Winter. (Jul. 2016). *Vorwurf Gegen Carsharing von BMW: Welche Daten Ihr Drive Now-Auto Sammelt und Was Damit Passieren Kann*. Accessed: Aug. 30, 2017. [Online]. Available: http://www.focus.de/5759933

[88] D. Eckhoff and C. Sommer, "Driving for big data? Privacy concerns in vehicular networking," *IEEE Security Privacy*, vol. 12, no. 1, pp. 77–79, Jan./Feb. 2014.

[89] J. J. Haas, Y.-C. Hu, and K. P. Laberteaux, "Efficient certificate revocation list organization and distribution," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 3, pp. 595–604, Mar. 2011.

[90] P. Knapik, E. Schoch, M. Müller, and F. Kargl, "Understanding vehicle related crime to elaborate on countermeasures based on ADAS and V2X communication," in *Proc. 4th IEEE Veh. Netw. Conf. (VNC)*, Seoul, South Korea, Nov. 2012, pp. 86–93.

[91] Leapcraft ApS. (2013). *CITS: Copenhagen Intelligent Traffic Solutions*. Accessed: Aug. 30, 2017. [Online]. Available: https://web.archive.org/web/20161019000247/http://leapcraft.dk:80/cits/

[92] I. Wagner and D. Eckhoff, "Technical privacy metrics: A systematic survey," *arXiv:1512.00327 [cs, math]*, Dec. 2015.

[93] I. Wagner, "Evaluating the strength of genomic privacy metrics," *ACM Trans. Privacy Security*, vol. 20, no. 1, Feb. 2017, Art. no. 2.

[94] C. Díaz, "Anonymity metrics revisited," in *Proc. Dagstuhl Seminar Anonymous Commun. Appl.*, Oct. 2005, pp. 1–6.

[95] I. Wagner and D. Eckhoff, "Privacy assessment in vehicular networks using simulation," in *Proc. Win. Simulat. Conf. (WSC)*, Savanah, GA, USA, Dec. 2014, pp. 3155–3166.

[96] S. Gürses, C. Troncoso, and C. Diaz, "Engineering privacy by design," in *Proc. 4th Int. Conf. Comput. Privacy Data Protect. (CPDP)*, Brussels, Belgium, Jan. 2011.

[97] A. Cavoukian, "Privacy by design—The 7 foundational principles," Inf. Privacy Commissioner Ontario, Toronto, ON, Canada, Tech. Rep., Jun. 2013. [Online]. Available: https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf

[98] S. Spiekermann, "The challenges of privacy by design," *Commun. ACM*, vol. 55, no. 7, pp. 38–40, Jul. 2012.

[99] D. Preuveneers and W. Joosen, "Privacy-enabled remote health monitoring applications for resource constrained wearable devices," in *Proc. 31st Annu. ACM Symp. Appl. Comput. (SAC)*, Pisa, Italy, Apr. 2016, pp. 119–124.

[100] A. Kung, J.-C. Freytag, and F. Kargl, "Privacy-by-design in its applications," in *Proc. IEEE Int. Symp. World Wireless Mobile Multimedia Netw. (WoWMoM)*, Lucca, Italy, Jun. 2011, pp. 1–6.

[101] J.-H. Hoepman, "Privacy design strategies," in *ICT Systems Security and Privacy Protection (SEC)*. Heidelberg, Germany: Springer, Jun. 2014, pp. 446–459.

[102] C. Kalloniatis, E. Kavakli, and S. Gritzalis, "Addressing privacy requirements in system design: The PriS method," *Requirements Eng.*, vol. 13, no. 3, pp. 241–255, Sep. 2008.

[103] M. Deng, K. Wuyts, R. Scandariato, B. Preneel, and W. Joosen, "A privacy threat analysis framework: Supporting the elicitation and fulfillment of privacy requirements," *Requirements Eng.*, vol. 16, no. 1, pp. 3–32, Mar. 2011.

[104] K. Beckers, "Comparing privacy requirements engineering approaches," in *Proc. 7th Int. Conf. Availability Rel. Security (ARES)*, Prague, Czechia, Aug. 2012, pp. 574–581.

[105] S. Spiekermann and L. F. Cranor, "Engineering privacy," *IEEE Trans. Softw. Eng.*, vol. 35, no. 1, pp. 67–82, Jan./Feb. 2009.

[106] *Privacy Requirements Definition and Testing*, MITRE Corporat., McLean, VA, USA, Mar. 2016, accessed: Aug. 30, 2017. [Online]. Available: https://www.mitre.org/publications/systems-engineering-guide/enterprise-engineering/engineering-informationintensive

[107] J. Jung *et al.*, "Privacy Oracle: A system for finding application leaks with black box differential testing," in *Proc. 15th ACM Conf. Comput. Commun. Security (CCS)*, Alexandria, VA, USA, Oct. 2008, pp. 279–288.

[108] S. McCamant and M. D. Ernst, "Quantitative information flow as network flow capacity," in *Proc. 29th ACM SIGPLAN Conf. Program. Lang. Design Implement. (PLDI)*, Tucson, AZ, USA, Jun. 2008, pp. 193–205.

[109] W. Enck *et al.*, "TaintDroid: An information-flow tracking system for realtime privacy monitoring on smartphones," *ACM Trans. Comput. Syst.*, vol. 32, no. 2, pp. 1–29, Jun. 2014.

[110] S. Delaune, M. Ryan, and B. Smyth, "Automatic verification of privacy properties in the applied pi calculus," in *Proc. Joint iTrust PST Conf. Privacy Trust Manag. Security (IFIPTM)*, Trondheim, Norway, Jun. 2008, pp. 263–278.

[111] M. Kost, J.-C. Freytag, F. Kargl, and A. Kung, "Privacy verification using ontologies," in *Proc. 6th Int. Conf. Availability Rel. Security (ARES)*, Vienna, Austria, Aug. 2011, pp. 627–632.

[112] F. Amato and F. Moscato, "A model driven approach to data privacy verification in e-health systems," *Trans. Data Privacy*, vol. 8, no. 3, pp. 273–296, Dec. 2015.

[113] O. Tene and J. Polonetsky, "Big data for all: Privacy and user control in the age of analytics," *Northwestern J. Technol. Intellectual Property*, vol. 11, no. 5, p. 239, Apr. 2013.

[114] Chaos Computer Club. (Jan. 2010). *Datenbrief*. Accessed: Aug. 30, 2017. [Online]. Available: https://www.ccc.de/en/datenbrief

[115] M. Janic, J. P. Wijbenga, and T. Veugen, "Transparency enhancing tools (TETs): An overview," in *Proc. IEEE Comput. Security Found. Symp. (CSF) 3rd Int. Workshop Socio Tech. Aspects Security Trust (STAST)*, New Orleans, LA, USA, Jun. 2013, pp. 18–25.

[116] N. Diakopoulos, "Accountability in algorithmic decision making," *Commun. ACM*, vol. 59, no. 2, pp. 56–62, Feb. 2016.

[117] J. Singh, T. F. J.-M. Pasquier, and J. Bacon, "Securing tags to control information flows within the Internet of Things," in *Proc. Int. Conf. Recent Adv. Internet Things (RioT)*, Singapore, Apr. 2015, pp. 1–6.

[118] D. Garg, L. Jia, and A. Datta, "Policy auditing over incomplete logs: Theory, implementation and applications," in *Proc. 18th ACM Conf. Comput. Commun. Security (CCS)*, Chicago, IL, USA, Oct. 2011, pp. 151–162.

[119] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for data storage security in cloud computing," in *Proc. IEEE INFOCOM*, San Diego, CA, USA, May 2010, pp. 1–9.

[120] A. Cavoukian, "Privacy and drones: Unmanned aerial vehicles," Inf. Privacy Commissioner Ontario, Toronto, ON, Canada, Tech. Rep., Aug. 2012. [Online]. Available: https://www.ipc.on.ca/wp-content/uploads/Resources/pbd-drones.pdf

[121] H. Choi, S. Chakraborty, Z. M. Charbiwala, and M. B. Srivastava, "SensorSafe: A framework for privacy-preserving management of personal sensory information," in *Secure Data Management* (LNCS 6933). Heidelberg, Germany: Springer, Sep. 2011, pp. 85–100.

[122] M. Layouni, K. Verslype, M. T. Sandıkkaya, B. D. Decker, and H. Vangheluwe, "Privacy-preserving telemonitoring for eHealth," in *Data and Applications Security XXIII* (LNCS 5645). Heidelberg, Germany: Springer, Jul. 2009, pp. 95–110.

[123] D. Le Métayer, "Privacy by design: A formal framework for the analysis of architectural choices," in *Proc. 3rd ACM Conf. Data Appl. Security Privacy (CODASPY)*, San Antonio, TX, USA, Feb. 2013, pp. 95–104.

[124] A. Monreale, S. Rinzivillo, F. Pratesi, F. Giannotti, and D. Pedreschi, "Privacy-by-design in big data analytics and social mining," *EPJ Data Sci.*, vol. 3, no. 1, p. 10, Sep. 2014.

[125] P. Samarati, "Protecting respondents identities in microdata release," *IEEE Trans. Knowl. Data Eng.*, vol. 13, no. 6, pp. 1010–1027, Nov./Dec. 2001.

[126] L. Sweeney, "K-anonymity: A model for protecting privacy," *Int. J. Uncertainty Fuzziness Knowl. Based Syst.*, vol. 10, no. 5, pp. 557–570, Oct. 2002.

[127] N. Li, W. Qardaji, and D. Su, "On sampling, anonymization, and differential privacy or, K-anonymization meets differential privacy," in *Proc. 7th ACM Symp. Inf. Comput. Commun. Security (ASIACCS)*, Seoul, South Korea, May 2012, pp. 32–33.

[128] A. Machanavajjhala, D. Kifer, J. Gehrke, and M. Venkitasubramaniam, "L-diversity: Privacy beyond k-anonymity," *ACM Trans. Knowl. Disc. Data*, vol. 1, no. 1, Mar. 2007, Art. no. 3.

[129] X. Xiao and Y. Tao, "M-invariance: Towards privacy preserving re-publication of dynamic datasets," in *Proc. ACM SIGMOD Int. Conf. Manag. Data*, Beijing, China, Jun. 2007, pp. 689–700.

[130] N. Li, T. Li, and S. Venkatasubramanian, "T-closeness: Privacy beyond k-anonymity and l-diversity," in *Proc. 23rd Int. Conf. Data Eng. (ICDE)*, Istanbul, Turkey, Jun. 2007, pp. 106–115.

[131] B. C. M. Fung, K. Wang, R. Chen, and P. S. Yu, "Privacy-preserving data publishing: A survey of recent developments," *ACM Comput. Surveys*, vol. 42, no. 4, pp. 1–53, Jun. 2010.

[132] C. Dwork, "Differential privacy," in *Automata, Languages and Programming* (LNCS 4052). Heidelberg, Germany: Springer, Jul. 2006, pp. 1–12.

[133] C. Dwork, M. Naor, O. Reingold, G. N. Rothblum, and S. Vadhan, "On the complexity of differentially private data release: Efficient algorithms and hardness results," in *Proc. 41st ACM Symp. Theory Comput. (STOC)*, Bethesda, MD, USA, May 2009, pp. 381–390.

[134] G. Ács and C. Castelluccia, "I have a DREAM! (DiffeRentially privatE smArt Metering)," in *Information Hiding* (LNCS 6958). Heidelberg, Germany: Springer, May 2011, pp. 118–132.

[135] M. E. Andrés, N. E. Bordenabe, K. Chatzikokolakis, and C. Palamidessi, "Geo-indistinguishability: Differential privacy for location-based systems," in *Proc. 20th ACM Conf. Comput. Commun. Security (CCS)*, Berlin, Germany, Nov. 2013, pp. 901–914.

[136] D. Boneh and X. Boyen, "Efficient selective-ID secure identity based encryption without random Oracles," in *Advances in Cryptology—EUROCRYPT 2004* (LNCS 3027). Heidelberg, Germany: Springer, May 2004, pp. 223–238.

[137] D. J. Wu, A. Taly, A. Shankar, and D. Boneh, "Privacy, discovery, and authentication for the Internet of Things," in *Computer Security—ESORICS 2016* (LNCS 9879). Cham, Switzerland: Springer, Sep. 2016, pp. 301–319.

[138] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proc. 13th ACM Conf. Comput. Commun. Security (CCS)*, Alexandria, VA, USA, Nov. 2006, pp. 89–98.

[139] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption," *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 1, pp. 131–143, Jan. 2013.

[140] J. Zhou, X. Lin, X. Dong, and Z. Cao, "PSMPA: Patient self-controllable and multi-level privacy-preserving cooperative authentication in distributed m-healthcare cloud computing system," *IEEE Trans. Parallel Distrib. Syst.*, vol. 26, no. 6, pp. 1693–1703, Jun. 2015.

[141] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *Advances in Cryptology—EUROCRYPT'99* (LNCS 1592). Heidelberg, Germany: Springer, May 1999, pp. 223–238.

[142] T. Elgamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Trans. Inf. Theory*, vol. IT-31, no. 4, pp. 469–472, Jul. 1985.

[143] C. Gentry, "Fully homomorphic encryption using ideal lattices," in *Proc. 41st ACM Symp. Theory Comput. (STOC)*, Bethesda, MD, USA, Jun. 2009, pp. 169–178.

[144] W. Dai, Y. Doroz, and B. Sunar, "Accelerating NTRU based homomorphic encryption using GPUs," in *Proc. IEEE High Perform. Extreme Comput. Conf. (HPEC)*, Waltham, MA, USA, Sep. 2014, pp. 1–6.

[145] E. De Cristofaro, S. Faber, P. Gasti, and G. Tsudik, "Genodroid: Are privacy-preserving genomic tests ready for prime time?" in *Proc. 19th ACM Conf. Comput. Commun. Security (CCS) 11th Workshop Privacy Electron. Soc. (WPES)*, Bethesda, MD, USA, Oct. 2012, pp. 97–108.

[146] Z. Erkin, T. Veugen, T. Toft, and R. Lagendijk, "Generating private recommendations efficiently using homomorphic encryption and data packing," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 3, pp. 1053–1066, Jun. 2012.

[147] S. Goldwasser, S. Micali, and C. Rackoff, "The knowledge complexity of interactive proof systems," *SIAM J. Comput.*, vol. 18, no. 1, pp. 186–208, Feb. 1989.

[148] J.-J. Quisquater, L. Guillou, M. Annick, and T. Berson, "How to explain zero-knowledge protocols to your children," in *Proc. Conf. Theory Appl. Cryptol. (CRYPTO)*, vol. 435. Santa Barbara, CA, USA, Aug. 1989, pp. 628–631.

[149] M. Jawurek, M. Johns, and F. Kerschbaum, "Plug-in privacy for smart metering billing," in *Privacy Enhancing Technologies* (LNCS 6794). Heidelberg, Germany: Springer, Jul. 2011, pp. 192–210.

[150] J. Balasch *et al.*, "PrETP: Privacy-preserving electronic toll pricing," in *Proc. 19th USENIX Security Symp.*, Washington, DC, USA, Aug. 2010, pp. 63–78.

[151] A. Shamir, "How to share a secret," *Commun. ACM*, vol. 22, no. 11, pp. 612–613, Nov. 1979.

[152] J. Shi, R. Zhang, Y. Liu, and Y. Zhang, "PriSense: Privacy-preserving data aggregation in people-centric urban sensing systems," in *Proc. 29th IEEE Conf. Comput. Commun. (INFOCOM)*, San Diego, CA, USA, Mar. 2010, pp. 758–766.

[153] K. Kursawe, G. Danezis, and M. Kohlweiss, "Privacy-friendly aggregation for the smart-grid," in *Privacy Enhancing Technologies* (LNCS 6794). Heidelberg, Germany: Springer, Jul. 2011, pp. 175–191.

[154] Q. Wang, K. Ren, S. Yu, and W. Lou, "Dependable and secure sensor data storage with dynamic integrity assurance," *ACM Trans. Sensor Netw.*, vol. 8, no. 1, pp. 1–24, Aug. 2011.

[155] D. Förster, H. Löhr, and F. Kargl, "Decentralized enforcement of k-anonymity for location privacy using secret sharing," in *Proc. IEEE Veh. Netw. Conf. (VNC)*, Kyoto, Japan, Dec. 2015, pp. 279–286.

[156] D. Chaum, "Blind signatures for untraceable payments," in *Advances in Cryptology*, D. Chaum, R. L. Rivest, and A. T. Sherman, Eds. Boston, MA, USA: Springer, 1983, pp. 199–203.

[157] F. Schaub, F. Kargl, Z. Ma, and M. Weber, "V-tokens for conditional pseudonymity in VANETs," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Sydney, NSW, Australia, Apr. 2010, pp. 1–6.

[158] J. Camenisch and A. Lysyanskaya, "An efficient system for non-transferable anonymous credentials with optional anonymity revocation," in *Advances in Cryptology—EUROCRYPT 2001* (LNCS 2045). Heidelberg, Germany: Springer, May 2001, pp. 93–118.

[159] J. Camenisch *et al.*, "Concepts and languages for privacy-preserving attribute-based authentication," in *Proc. IFIP Working Conf. Policies Res. Identity Manag. (IDMAN)*, vol. 396. London, U.K., Apr. 2013, pp. 34–52.

[160] J. Petit, F. Schaub, M. Feiri, and F. Kargl, "Pseudonym schemes in vehicular networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 1, pp. 228–255, 1st Quart., 2015.

[161] E. Brickell, J. Camenisch, and L. Chen, "Direct anonymous attestation," in *Proc. 11th ACM Conf. Comput. Commun. Security (CCS)*, Washington, DC, USA, Oct. 2004, pp. 132–145.

[162] A. C. Yao, "Protocols for secure computations," in *Proc. 23rd Annu. Symp. Found Comput. Sci. (SFCS)*, Chicago, IL, USA, Nov. 1982, pp. 160–164.

[163] P. Bogetoft *et al.*, "Secure multiparty computation goes live," in *Financial Cryptography and Data Security* (LNCS 5628). Heidelberg, Germany: Springer, Feb. 2009, pp. 325–343.

[164] S. Jha, L. Kruger, and V. Shmatikov, "Towards practical privacy for genomic computation," in *Proc. IEEE Symp. Security Privacy*, Oakland, CA, USA, May 2008, pp. 216–230.

[165] C. Devet, I. Goldberg, and N. Heninger, "Optimally robust private information retrieval," in *Proc. 21st USENIX Security Symp.*, Bellevue, WA, USA, Aug. 2012, pp. 269–283.

[166] C. Devet and I. Goldberg, "The best of both worlds: Combining information-theoretic and computational PIR for communication efficiency," in *Privacy Enhancing Technologies* (LNCS 8555). Cham, Switzerland: Springer, Jul. 2014, pp. 63–82.

[167] P. Williams, R. Sion, and B. Carbunar, "Building castles out of mud: Practical access pattern privacy and correctness on untrusted storage," in *Proc. 15th ACM Conf. Comput. Commun. Security (CCS)*, Alexandria, VA, USA, Oct. 2008, pp. 139–148.

[168] S. Ravi, A. Raghunathan, P. Kocher, and S. Hattangady, "Security in embedded systems: Design challenges," *ACM Trans. Embedded Comput. Syst.*, vol. 3, no. 3, pp. 461–491, Aug. 2004.

[169] N. Komninos, E. Philippou, and A. Pitsillides, "Survey in smart grid and smart home security: Issues, challenges and countermeasures," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 4, pp. 1933–1954, 4th Quart., 2014.

[170] M. La Polla, F. Martinelli, and D. Sgandurra, "A survey on security for mobile devices," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 1, pp. 446–471, 1st Quart., 2013.

[171] A. P. Felt, M. Finifter, E. Chin, S. Hanna, and D. Wagner, "A survey of mobile malware in the wild," in *Proc. 18th ACM Conf. Comput. Commun. Security (CCS) 1st ACM Workshop Security Privacy Smartphones Mobile Devices (SPSM)*, Chicago, IL, USA, Oct. 2011, pp. 3–14.

[172] A. S. Uluagac, V. Subramanian, and R. Beyah, "Sensory channel threats to cyber physical systems: A wake-up call," in *Proc. IEEE Conf. Commun. Netw. Security (CNS)*, San Francisco, CA, USA, Oct. 2014, pp. 301–309.

[173] J. Petit, B. Stottelaar, M. Feiri, and F. Kargl, "Remote attacks on automated vehicles sensors: Experiments on camera and LiDAR," in *Proc. Black Hat Europe*, vol. 11. 2015.

[174] T. F. J.-M. Pasquier, J. Singh, D. Eyers, and J. Bacon, "CamFlow: Managed data-sharing for cloud services," *IEEE Trans. Cloud Comput.*, vol. 5, no. 3, pp. 472–484, Jul./Sep. 2017.

[175] D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Trans. Inf. Theory*, vol. IT-29, no. 2, pp. 198–208, Mar. 1983.

[176] C. Hennebert and J. Dos Santos, "Security protocols and privacy issues into 6LoWPAN stack: A synthesis," *IEEE Internet Things J.*, vol. 1, no. 5, pp. 384–398, Oct. 2014.

[177] P. McDaniel and S. McLaughlin, "Security and privacy challenges in the smart grid," *IEEE Security Privacy*, vol. 7, no. 3, pp. 75–77, May/Jun. 2009.

[178] K. Zhao and L. Ge, "A survey on the Internet of Things security," in *Proc. 9th Int. Conf. Comput. Intell. Security (CIS)*, Leshan, China, Dec. 2013, pp. 663–667.

[179] B. Bloessl, C. Sommer, F. Dressler, and D. Eckhoff, "The scrambler attack: A robust physical layer attack on location privacy in vehicular networks," in *Proc. Int. Conf. Comput. Netw. Commun. (ICNC)*, Garden Grove, CA, USA, Feb. 2015, pp. 395–400.

[180] J. Han, E. Owusu, L. T. Nguyen, A. Perrig, and J. Zhang, "ACComplice: Location inference using accelerometers on smartphones," in *Proc. 4th Int. Conf. Commun. Syst. Netw. (COMSNETS)*, Bengaluru, India, Jan. 2012, pp. 1–9.

[181] J. D. Barnes, P. H. Distler, and M. P. McMullen, "Location inference using radio frequency fingerprinting," U.S. Patent 7 945 271, May 2011.

[182] M. Georgiev *et al.*, "The most dangerous code in the world: Validating SSL certificates in non-browser software," in *Proc. 19th Conf. Comput. Commun. Security (CCS)*, Raleigh, NC, USA, Oct. 2012, pp. 38–49.

[183] S. Fahl *et al.*, "Why eve and Mallory love android: An analysis of android SSL (in)security," in *Proc. 19th Conf. Comput. Commun. Security (CCS)*, Raleigh, NC, USA, Oct. 2012, pp. 50–61.

[184] B. He *et al.*, "Vetting SSL usage in applications with SSLINT," in *Proc. IEEE Symp. Security Privacy*, San Jose, CA, USA, May 2015, pp. 519–534.

[185] A. Bates *et al.*, "Securing SSL certificate verification through dynamic linking," in *Proc. 21st Conf. Comput. Commun. Security (CCS)*, Scottsdale, AZ, USA, Nov. 2014, pp. 394–405.

[186] X. Lin, R. Lu, X. Shen, Y. Nemoto, and N. Kato, "Sage: A strong privacy-preserving scheme against global eavesdropping for eHealth systems," *IEEE J. Sel. Areas Commun.*, vol. 27, no. 4, pp. 365–378, May 2009.

[187] R. Dingledine, N. Mathewson, and P. Syverson, "Tor: The second-generation onion router," in *Proc. 13th USENIX Security Symp.*, San Diego, CA, USA, Aug. 2004, p. 21.

[188] E. Erdin, C. Zachor, and M. H. Gunes, "How to find hidden users: A survey of attacks on anonymity networks," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 2296–2316, 4th Quart., 2015.

[189] A. Johnson, C. Wacek, R. Jansen, M. Sherr, and P. Syverson, "Users get routed: Traffic correlation on Tor by realistic adversaries," in *Proc. 20th Conf. Comput. Commun. Security (CCS)*, Berlin, Germany, Nov. 2013, pp. 337–348.

[190] B. N. Levine, M. K. Reiter, C. Wang, and M. Wright, "Timing attacks in low-latency mix systems," in *Financial Cryptography* (LNCS 3110). Heidelberg, Germany: Springer, Feb. 2004.

[191] N. Nikiforakis *et al.*, "Cookieless monster: Exploring the ecosystem of Web-based device fingerprinting," in *Proc. IEEE Symp. Security Privacy*, Berkeley, CA, USA, May 2013, pp. 541–555.

[192] T. Kohno, A. Broido, and K. C. Claffy, "Remote physical device fingerprinting," *IEEE Trans. Depend. Secure Comput.*, vol. 2, no. 2, pp. 93–108, Apr./Jun. 2005.

[193] C. Neumann, O. Heen, and S. Onno, "An empirical study of passive 802.11 device fingerprinting," in *Proc. 32nd Int. Conf. Distrib. Comput. Syst. Workshops*, Macau, China, Jun. 2012, pp. 593–602.

[194] M. Gruteser and D. Grunwald, "Enhancing location privacy in wireless LAN through disposable interface identifiers: A quantitative analysis," *Mobile Netw. Appl.*, vol. 10, no. 3, pp. 315–325, Jun. 2005.

[195] N. Nikiforakis, W. Joosen, and B. Livshits, "PriVaricator: Deceiving fingerprinters with little white lies," in *Proc. 24th Int. Conf. World Wide Web (WWW)*, Florence, Italy, May 2015, pp. 820–830.

[196] T. Wang, X. Cai, R. Nithyanand, R. Johnson, and I. Goldberg, "Effective attacks and provable defenses for website fingerprinting," in *Proc. 23rd USENIX Security Symp.*, San Diego, CA, USA, Aug. 2014, pp. 143–157.

[197] B. Danev, D. Zanetti, and S. Capkun, "On physical-layer identification of wireless devices," *ACM Comput. Surveys*, vol. 45, no. 1, pp. 1–29, Dec. 2012.

[198] C. Xenakis and C. Ntantogian, "Attacking the baseband modem of mobile phones to breach the users' privacy and network security," in *Proc. 7th Int. Conf. Cyber Conflict Archit. Cyberspace*, Tallinn, Estonia, May 2015, pp. 231–244.

[199] A. P. Felt *et al.*, "Android permissions: User attention, comprehension, and behavior," in *Proc. 18th Symp. Usable Privacy Security (SOUPS)*, Washington, DC, USA, Jul. 2012, pp. 1–14.

[200] City of Chicago. (2016). *The Broadband Challenge*. Accessed: Aug. 30, 2017. [Online]. Available: http://digital.cityofchicago.org/index.php/the-broadband-challenge/

[201] Privacy International. (Mar. 2016). *The Right to Privacy in Estonia*. Accessed: Aug. 30, 2017. [Online]. Available: https://www.privacyinternational.org/sites/default/files/HRC_estonia.pdf

[202] Meta Mesh Wireless Communities. (2016). *Meta Mesh | Wireless Networking for All*. Accessed: Aug. 30, 2017. [Online]. Available: http://www.metamesh.org

[203] G. Madlmayr, J. Langer, C. Kantner, and J. Scharinger, "NFC devices: Security and privacy," in *Proc. 3rd Int. Conf. Availability Rel. Security (ARES)*, Barcelona, Spain, Mar. 2008, pp. 642–647.

[204] J. R. Troncoso-Pastoriza, D. González-Jiménez, and F. Pérez-González, "Fully private noninteractive face verification," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 7, pp. 1101–1114, Jul. 2013.

[205] D. Christin, A. Reinhardt, S. S. Kanhere, and M. Hollick, "A survey on privacy in mobile participatory sensing applications," *J. Syst. Softw.*, vol. 84, no. 11, pp. 1928–1946, Nov. 2011.

[206] A. Raij, A. Ghosh, S. Kumar, and M. Srivastava, "Privacy risks emerging from the adoption of innocuous wearable sensors in the mobile environment," in *Proc. SIGCHI Conf. Human Factors Comput. Syst. (CHI)*, Vancouver, BC, Canada, May 2011, pp. 11–20.

[207] *Intelligent Transport Systems (ITS); Security; Trust and Privacy Management*, ETSI Standard TS 102 941 V1.1.1, Jun. 2012.

[208] C.-Y. Chow, M. F. Mokbel, and T. He, "A privacy-preserving location monitoring system for wireless sensor networks," *IEEE Trans. Mobile Comput.*, vol. 10, no. 1, pp. 94–107, Jan. 2011.

[209] H. Wu and Y.-C. Hu, "Location privacy with randomness consistency," *Proc. Privacy Enhanc. Technol.*, vol. 2016, no. 4, pp. 62–82, Oct. 2016.

[210] J. Cao, B. Carminati, E. Ferrari, and K.-L. Tan, "CASTLE: Continuously anonymizing data streams," *IEEE Trans. Depend. Secure Comput.*, vol. 8, no. 3, pp. 337–352, May/Jun. 2011.

[211] C. Dwork and A. Roth, *The Algorithmic Foundations of Differential Privacy*. Boston, MA, USA: Now, Aug. 2014.

[212] C. Culnane, B. I. P. Rubinstein, and V. Teague, "Privacy assessment of de-identified opal data: A report for transport for NSW," *arXiv:1704.08547 [cs]*, Apr. 2017.

[213] K. Chatzikokolakis, C. Palamidessi, and M. Stronati, "Constructing elastic distinguishability metrics for location privacy," *Proc. Privacy Enhanc. Technol.*, vol. 2015, no. 2, pp. 156–170, Jun. 2015.

[214] M. Li, W. Lou, and K. Ren, "Data security and privacy in wireless body area networks," *IEEE Wireless Commun.*, vol. 17, no. 1, pp. 51–58, Feb. 2010.

[215] O. G. Morchon and H. Baldus, "Efficient distributed security for wireless medical sensor networks," in *Proc. Int. Conf. Intell. Sensors Sensor Netw. Inf. Process. (ISSNIP)*, Sydney, NSW, Australia, Dec. 2008, pp. 249–254.

[216] C. Castelluccia, E. Mykletun, and G. Tsudik, "Efficient aggregation of encrypted data in wireless sensor networks," in *Proc. 2nd Annu. Int. Conf. Mobile Ubiquitous Syst. Netw. Services (MobiQuitous)*, San Diego, CA, USA, Jul. 2005, pp. 109–117.

[217] F. D. Garcia and B. Jacobs, "Privacy-friendly energy-metering via homomorphic encryption," in *Security and Trust Management* (LNCS 6710). Heidelberg, Germany: Springer, Sep. 2010, pp. 226–238.

[218] C. Patsakis, P. Laird, M. Clear, M. Bouroche, and A. Solanas, "Interoperable privacy-aware e-participation within smart cities," *Computer*, vol. 48, no. 1, pp. 52–58, Jan. 2015.

[219] M.-P. Pelletier, M. Trépanier, and C. Morency, "Smart card data use in public transit: A literature review," *Transp. Res. C Emerg. Technol.*, vol. 19, no. 4, pp. 557–568, Aug. 2011.

[220] D. Eckhoff, C. Sommer, F. Dressler, R. German, and T. Gansen, "SlotSwap: Strong and affordable location privacy in intelligent transportation systems," *IEEE Commun. Mag.*, vol. 49, no. 11, pp. 126–133, Nov. 2011.

[221] D. Eckhoff and C. Sommer, "Marrying safety with privacy: A holistic solution for location privacy in VANETs," in *Proc. 8th IEEE Veh. Netw. Conf. (VNC)*, Columbus, OH, USA, Dec. 2016, pp. 1–8.

[222] D. Eckhoff, F. Dressler, and C. Sommer, "SmartRevoc: An efficient and privacy preserving revocation system using parked vehicles," in *Proc. 38th IEEE Conf. Local Comput. Netw. (LCN)*, Sydney, NSW, Australia, Oct. 2013, pp. 855–862.

[223] A. Ben-David, N. Nisan, and B. Pinkas, "FairplayMP: A system for secure multi-party computation," in *Proc. 15th Conf. Comput. Commun. Security (CCS)*, Alexandria, VA, USA, Oct. 2008, pp. 257–266.

[224] C. C. Aggarwal and P. S. Yu, "A general survey of privacy-preserving data mining models and algorithms," in *Privacy-Preserving Data Mining* (Advances in Database Systems), vol. 32. Boston, MA, USA: Springer, 2008, pp. 11–52.

[225] G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, and K.-L. Tan, "Private queries in location based services: Anonymizers are not necessary," in *Proc. SIGMOD Int. Conf. Manag. Data*, Vancouver, BC, Canada, Jun. 2008, pp. 121–132.

[226] P. Golle and K. Partridge, "On the anonymity of home/work location pairs," in *Pervasive Computing* (LNCS 5538). Heidelberg, Germany: Springer, May 2009, pp. 390–397.

[227] Ayuntamiento de Zaragoza. (2016) *Tarjeta Ciudadana*. Accessed: Aug. 30, 2017. [Online]. Available: http://www.zaragoza.es/ciudad/sectores/tarjetaciudadana/

[228] M. Shukri and M. Hafiz, "The privacy and security of an identification card: Malaysian perspective," Faculty Econ. Bus., Universiti Malaysia Sarawak, Kota Samarahan, Malaysia, Tech. Rep. 65855, Jul. 2015.

[229] Y. A. Kee, Y. C. Nee, L. Y. Beng, and T. S. Fun, "Security issues on identity card in Malaysia," *Int. J. Eng. Technol.*, vol. 4, no. 5, pp. 617–621, Oct. 2012.

[230] D. Leoni, "Non-interactive differential privacy: A survey," in *Proc. 21st Int. World Wide Web Conf. (WWW) 1st Int. Workshop Open Data (WOD)*, Nantes, France, May 2012, pp. 40–52.

[231] Transport for NSW. (Apr. 2017). *Opal Tap on and Tap Off*. Accessed: Aug. 30, 2017. [Online]. Available: https://opendata.transport.nsw.gov.au/dataset/opal-tap-on-and-tap-off

[232] H. J. Asghar, P. Tyler, and M. A. Kaafar, "Differentially private release of public transport data: The opal use case," *arXiv:1705.05957 [cs]*, May 2017.

[233] S. Rynkiewicz. (Jul. 2015). *Private Data and Public Health: How Chicago Health Atlas Protects Identities*. Accessed: Aug. 30, 2017. [Online]. Available: http://www.smartchicagocollaborative.org/health-data-privacy-security/

[234] H. Xie, L. Kulik, and E. Tanin, "Privacy-aware traffic monitoring," *IEEE Trans. Intell. Transp. Syst.*, vol. 11, no. 1, pp. 61–70, Mar. 2010.

[235] R. Shokri, C. Troncoso, C. Diaz, J. Freudiger, and J.-P. Hubaux, "Unraveling an old cloak: K-anonymity for location privacy," in *Proc. 17th ACM Conf. Comput. Commun. Security (CCS) 9th Workshop Privacy Electron. Soc. (WPES)*, Chicago, IL, USA, Oct. 2010, pp. 115–118.

[236] Y. A. W. de Kort *et al.*, "De-escalate: Defusing escalating behaviour through the use of interactive light scenarios," in *Proc. Experiencing Light*, Eindhoven, The Netherlands, Nov. 2014, pp. 94–97.

[237] S. Wang *et al.*, "Security in wearable communications," *IEEE Netw.*, vol. 30, no. 5, pp. 61–67, Sep./Oct. 2016.

[238] S. S. Javadi and M. A. Razzaque, "Security and privacy in wireless body area networks for health care applications," in *Wireless Networks and Security*, S. Khan and A.-S. K. Pathan, Eds. Heidelberg, Germany: Springer, 2013, pp. 165–187.

[239] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, and A. Jamalipour, "A survey of routing attacks in mobile ad hoc networks," *IEEE Wireless Commun.*, vol. 14, no. 5, pp. 85–91, Oct. 2007.

[240] J. Granjal, E. Monteiro, and J. Sá Silva, "Security for the Internet of Things: A survey of existing protocols and open research issues," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 3, pp. 1294–1312, 3rd Quart., 2015.

[241] S. Finster and I. Baumgart, "Privacy-aware smart metering: A survey," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 2, pp. 1088–1101, 2nd Quart., 2015.

[242] C. Efthymiou and G. Kalogridis, "Smart grid privacy via anonymization of smart metering data," in *Proc. 1st Int. Conf. Smart Grid Commun. (SmartGridComm)*, Gaithersburg, MD, USA, Oct. 2010, pp. 238–243.

[243] G. Kalogridis, C. Efthymiou, S. Z. Denic, T. A. Lewis, and R. Cepeda, "Privacy for smart meters: Towards undetectable appliance load signatures," in *Proc. 1st Int. Conf. Smart Grid Commun. (SmartGridComm)*, Gaithersburg, MD, USA, Oct. 2010, pp. 232–237.

[244] A. M. Sabelli, T. Kanda, and N. Hagita, "A conversational robot in an elderly care center: An ethnographic study," in *Proc. 6th Int. Conf. Human Robot Interact. (HRI)*, Lausanne, Switzerland, Mar. 2011, pp. 37–44.

[245] A. Sharkey and N. Sharkey, "Granny and the robots: Ethical issues in robot care for the elderly," *Ethics Inf. Technol.*, vol. 14, no. 1, pp. 27–40, Mar. 2012.

[246] C.-W. Chang, J.-H. Lee, P.-Y. Chao, C.-Y. Wang, and G.-D. Chen, "Exploring the possibility of using humanoid robots as instructional tools for teaching a second language in primary school," *J. Educ. Technol. Soc.*, vol. 13, no. 2, pp. 13–24, Apr. 2010.

[247] M. Rajamani. (Jan. 2017). *A Crime-Fighting Robot That Looks Like R2-D2 Is Patrolling 10th Avenue*. Accessed: Aug. 30, 2017. [Online]. Available: https://www.dnainfo.com/new-york/20170119/chelsea/knightscope-crime-robot-marquee-nightclub-10th-avenue

[248] M. Boone. (Sep. 2016). *Hospital Employs Roving Robot As New Security 'Guard'*. Accessed: Aug. 30, 2017. [Online]. Available: http://cbs6albany.com/news/offbeat/hospital-employs-roving-robot-as-new-security-guard

[249] Sputnik. (Apr. 2016). *Educating Pepper: Japanese Robot Celebrates First Day at School*. Accessed: Aug. 30, 2017. [Online]. Available: https://sputniknews.com/asia/201604141038028652-pepper-robot-first-day-school/

[250] F. Tanaka *et al.*, "Pepper learns together with children: Development of an educational application," in *Proc. 15th Int. Conf. Humanoid Robots (Humanoids)*, Seoul, South Korea, Nov. 2015, pp. 270–275.

[251] J. Krumm, "Inference attacks on location tracks," in *Pervasive Computing* (LNCS 4480). Heidelberg, Germany: Springer, May 2007, pp. 127–143.

[252] T. Bachmann, K. Naab, G. Reichart, and M. Schraut, "Enhancing traffic safety with BMW's driver assistance approach connected drive," in *Proc. 7th World Congr. Intell. Transp. Syst.*, Turin, Italy, Nov. 2000, p. 14.

[253] R. Kirk, "Cars of the future: The Internet of Things in the automotive industry," *Netw. Security*, vol. 2015, no. 9, pp. 16–18, Sep. 2015.

[254] M. Werner *et al.*, "Cellular in-band modem solution for eCall emergency data transmission," in *Proc. 69th Veh. Technol. Conf. (VTC Spring)*, Barcelona, Spain, Apr. 2009, pp. 1–6.

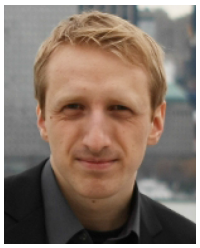
[255] Big Brother Watch. (Jul. 2014). *Mandatory Installation of Event Data Recorders: The eCall System*. Accessed: Aug. 30, 2017. [Online]. Available: https://www.bigbrotherwatch.org.uk/wp-content/uploads/2014/07/Briefing-Note-eCall-PDF.pdf

[256] *Toyota to Bring Vehicle-Infrastructure Cooperative Systems to New Models in 2015*, Toyota Motor Corporat., Toyota, Japan, Nov. 2014, accessed: Aug. 30, 2017. [Online]. Available: http://newsroom.toyota.co.jp/en/detail/4228471/

[257] *World's First Cooperative ITS Launched in Japan*, Toyota Motor Corporat., Toyota, Japan, Sep. 2015, accessed: Aug. 30, 2017. [Online]. Available: http://www.toyota-global.com/pages/contents/innovation/intelligent_transport_systems/world_congress/2015bordeaux/pdf/No3-4_Jitsuyoka_CooITS.pdf

[258] J. Henderson and J. Spencer, "Autonomous vehicles and commercial real estate," *Cornell Real Estate Rev.*, vol. 14, no. 1, pp. 44–55, Jun. 2016.

[259] Z. Xiao and Y. Xiao, "Security and privacy in cloud computing," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 2, pp. 843–859, 2nd Quart., 2013.
[260] *Privacy Engineering*, MITRE Corporat., McLean, VA, USA, 2013, accessed: Aug. 30, 2017. [Online]. Available: https://www.mitre.org/publications/systems-engineering-guide/enterprise-engineering/engineering-informationintensive-enterprises/privacy-systems-engineering
[261] S. Gürses and J. van Hoboken, "Privacy after the agile turn," in *The Cambridge Handbook of Consumer Privacy*, E. Selinger *et al.*, Eds. Cambridge, U.K.: Cambridge Univ. Press, 2017. [Online]. Available: https://osf.io/ufdvb/
[262] Z. Khan, Z. Pervez, and A. Ghafoor, "Towards cloud based smart cities data security and privacy management," in *Proc. 7th Int. Conf. Utility Cloud Comput. (UCC)*, London, U.K., Dec. 2014, pp. 806–811.
[263] M. H. Manshaei, Q. Zhu, T. Alpcan, T. Bacşar, and J.-P. Hubaux, "Game theory meets network security and privacy," *ACM Comput. Surveys*, vol. 45, no. 3, pp. 1–39, Jun. 2013.
[264] J. Bonneau *et al.*, "SoK: Research perspectives and challenges for bitcoin and cryptocurrencies," in *Proc. IEEE Symp. Security Privacy*, San Jose, CA, USA, May 2015, pp. 104–121.
[265] A. Dorri, S. S. Kanhere, and R. Jurdak, "Blockchain in Internet of Things: Challenges and solutions," *arXiv:1608.05187 [cs]*, Aug. 2016.
[266] G. Zyskind, O. Nathan, and A. S. Pentland, "Decentralizing privacy: Using blockchain to protect personal data," in *Proc. IEEE Security Privacy Workshops (SPW)*, San Jose, CA, USA, May 2015, pp. 180–184.
[267] S. Leman-Langlois, "Privacy as currency: Crime, information and control in cyberspace," in *Technocrime: Technology, Crime and Social Control*. Portland, OR, USA: Willan, Jul. 2008, pp. 112–138.
[268] D. Cvrcek, M. Kumpost, V. Matyas, and G. Danezis, "A study on the value of location privacy," in *Proc. 13th ACM Conf. Comput. Commun. Security (CCS) 5th Workshop Privacy Electron. Soc. (WPES)*, Alexandria, VA, USA, Oct. 2006, pp. 109–118.



David Eckhoff received the M.Sc. (Dipl.-Inf.Univ., graduating top of his class) degree in computer science and the Ph.D. (Dr.-Ing., with Distinction) degree in engineering from the University of Erlangen in 2009 and 2016, respectively. He is a Post-Doctoral Researcher with the Technical University of Munich and a Research Fellow with TUMCREATE, Singapore, a joint research institute by TU Munich and Nanyang Technological University, Singapore. In 2016, he was a Visiting Scholar with the group of Prof. L. Kulik with the University of Melbourne, Australia. In 2016, he joined TUMCREATE in Singapore in the group of Prof. A. Knoll. His research interests include privacy protection, smart cities, vehicular networks, and intelligent transportation systems with a particular focus on modeling and simulation.

Isabel Wagner received the M.Sc. (Dipl.-Inf.Univ.) degree in computer science and the Ph.D. (Dr.-Ing.) degree in engineering from the University of Erlangen in 2005 and 2010, respectively. She is a Senior Lecturer in computer science (Cybersecurity) with De Montfort University, Leicester, U.K. In 2011, she was a JSPS Post-Doctoral Fellow in the research group of M. Murata with Osaka University, Japan. Her research is focused on privacy and privacy-enhancing technologies, particularly on metrics to quantify the effectiveness of privacy protection mechanisms, as well as on privacy-enhancing technologies in genomics, smart cities, vehicular networks, and smart grids. She is also investigating bio-inspired mechanisms for privacy.