BIZCOMMUNITY

With smart cities, your every step will be recorded

By Sara Degli-Esposti and Siraj Ahmed Shaikh

18 Apr 2018

Modern cities are brimming with objects that receive, collect and transmit data. This includes mobile phones but also objects actually embedded into our cities, such as traffic lights and air pollution stations. Even something as simple as a garbage bin can now be connected to the internet, meaning that it forms part of what is called the internet of things (IoT).

Image source: www.pxhere.com

A smart city collects the data from these digital objects, and uses it to create new products and services that make cities more liveable.

Although they have huge potential to make life better, the possibility of increasingly smarter cities also raises serious privacy concerns. Through sensors embedded into our cities, and the smartphones in our pockets, smart cities will have the power to constantly identify where people are, who they are meeting and even perhaps what they are doing.

Following revelations that 87m people's Facebook data was allegedly breached and used to influence electoral voting behaviour, it is ever more important to properly scrutinise where our data goes and how it is used. Similarly, as more and more critical infrastructure falls victim to cyber-attacks, we need to consider that our cities are not only becoming smarter, they are also becoming more vulnerable to cyber-attacks.

Smarter cities

Across the world, cities are rapidly becoming smarter. Cities as different as Singapore, London and San Francisco use technologies such as urban sensing (which captures how people interact with each other and their surroundings), geo-tracking (which records the movement of people), and real-time analytics (which processes the vast amount of collected data). Smart cities use these technologies to better manage energy and water supply, reduce contamination and traffic jams, optimise garbage collection routes or help people park their cars. A good example is Chicago's Array of Things project.

Smart city initiatives don't just have the potential to help make life more liveable, they can help us better the world. In 2013, the Greek academic Vassilis Kostakos introduced interactive LCD screens which encouraged people waiting at a bus stop to help identify malaria-infected blood cells.

Big data and privacy concerns

In the last few months, following the Cambridge Analytica and Facebook revelations, concerns over how companies use accumulated data has grown exponentially.

Back in 2009, experts were already aware that stakeholders could collect personal information from unaware users. Opaque privacy policies and complex data-sharing agreements allowed companies to bypass data protection law and use collected data for undeclared purposes.

Because of the huge and detailed information collected by internet of things (IoT) devices, smart city projects could lead to similar worries. Take for example, the Cityware project, which demonstrated the possibility of mapping not just digital but also physical encounters between Facebook friends. Cityware were able to track the movement and interaction of 30,000 people using their Facebook profile and smartphone bluetooth signals.

Smartphones collect a huge amount of data. Kristian Design/Pixabay, CC BY

Most people tend to underestimate that the smartphone they carry around is a very powerful sensing tool. In order to function, your phone continuously shares data about your location, digital and physical interaction, and more. When this data is matched with further information collected from IoT devices and smart grids – electricity supply networks that rapidly detect and react to local changes in usage – it raises serious implications for people's privacy and right to self determination.

Just as you give Facebook the right to own anything you post on your profile, the data collected by online sensors across smart cities will be owned by a variety of corporations, including internet service providers (ISPs). Last year, the US Congress overturned internet privacy protection by granting ISPs the right to sell users' information, such as browsing history, to third parties.

Once most of your gadgets are connected to the internet, the same objects could inform companies what brands and products you like and how and when you use them. This means that all the data which IoT gadgets will collect, whether in your home or in your city, potentially can be sold to third parties.

Cyber security worries

As cities get smarter, our digital information becomes even more vulnerable to cyber-attacks. For example, ransomware, which encrypts information and then asks for a ransom to free it, can hit even the biggest data holders, such as the UK National Health Service (NHS).

Stakes are extremely high when viruses hit local authorities. The recent cyber-attack on the city of Atlanta crippled several critical systems across the city, including the police department. Europol's No More Ransom! initiative gives good advice on how to deal with this type of threat.

Atlanta suffered ransomware attacks in 2018. Pixabay, CC BY

Hackers can take control of entire buildings or systems. The power blackout that left more than 225,000 people without light in Ukraine in December 2015 is an example. Working out who is responsible for a cyber-attack is always challenging but Russia was indicated as a potential suspect.

Ultimately, even with these concerns, embedding IoT into cities is a growing trend. To take control of what that means, people need to become better informed and more involved. The business models of stakeholders need to be scrutinised and their use of data needs to be accountable. Most of all, citizens need to be listened to on how they want their cities to develop.

ABOUT THE AUTHOR

Sara Degli-Esposti, research fellow, Coventry University. Siraj Ahmed Shaikh, professor of systems security, Coventry University.