Exposed: Privacy, Security and the Smart City

Shachi Sayata
TECHNEWS WRITER

Smart cities, by definition, are urban ecosystems that utilize digital networks and communication technologies to enhance the quality and performance of urban services and engage more effectively and actively with its citizens. Kent College of Law had a conference organized to understand the influence of privacy and security in a smart city. With Mayor Rahm Emanuel's launch of Chicago's first ever technology plan, it is imperative for us, as citizens, to understand the aspects that really go into making the city 'smart' today and how will we capitalize on the ubiquitous collection of data in the future while still maintaining sufficient aspects of privacy.

Are smart cities a necessity? What does it really mean to be under surveillance all the time? What is the cost associated with this surveillance? How secure is our data? Is there any scope for subjectivity in a smart city? These were a few questions that were analyzed during the conference. Though the concept of a smart city may only exist in our imagination today, such a hyperlinked network is soon to become a reality. Kent College of Law therefore decided to organize a conference and invite industry experts to answer these questions.

Adam Greenfield, who is a renowned writer, spoke about "networked urbanism" and influence of computer interactions in our everyday activities. He explained how network information technologies today utilize data for a wide array of activities from marketing initiatives to account for housing and mobility. The most interesting point he raised what that these technologies are not able to account for about one-third of the population, which largely consists of people who do not have access to the "smart infrastructure:" in essence, people who do not have a smartphone or computer and are thus not producing the data in ordered to be accounted for. Further, he explained how with increase in focus on data collection and data analytics energy utilization costs would increase drastically and therefore, there is a need to understand the long-term financial viability and sustainability of such an initiative. He cited an example of how by moving to a more "networked" environment women from a slum in India were able to map their locality without any sophisticated GPS device. This mapping was aimed to ensure that the city officials understood the region well and took necessary initiatives for improving the standard of living of people in the region.

Woodrow Hartzog, distinguished law professor at Stanford University, spoke about privacy in the hyperlinked network of the smart cities. Hartzog highlighted three key aspects related to privacy: obscurity, anonymity and trust. He was able to develop an interesting relationship between what is really private in the Internet ecosystem. We believe something is private because we assume that not many people will understand it. He emphasized the importance of how we should start thinking of our activities in public since, all the data we produce is captured, stored and analyzed. The most interesting point he raised was the question "are our faces private?" With the increase of surveillance using CCTV cameras in smart cities, can we safely assume that our faces are private? He later explained how in today's data system, "harm" is a very difficult aspect to articulate. Governments should thus focus their efforts on gaining trust of citizens and providing them with an opt-out mechanism wherever possible. Trust, as he stated, is dependent on discretion, honesty, protection and also ensures that those that collect the data from the subjects should be loyal to their subjects and act in their best interest.

Kimerly Bailey, who is a law professor at Kent College of Law, focused her discussion on the importance of privacy and how deprivation of privacy leads to devastating effects on social control. She described how constant monitoring of people of color by the state leads to a chilling effect. This has an impact on their freedom of association and self-expression. She cited instances of where stop-and-frisks have an impact on the social capital of an individual. Since these stops question the individual regarding his activities, they express a lack of trust and suspicion in the person. On some occasions, the police officials not only ask for personal information, but may also go through their belongings. This is usually carried out in public, thus, there is a feeling of shame associated with it. It inflicts a person's freedom of association since nobody would want to associate with a person who is subjected to frequent stop-and-frisks. In many regions, victims of these frisks have changed the way they dress in order to look less vulnerable. She advocated that before we promote more surveillance to improve security, we must be mindful of the chilling effects associated with this surveillance.

Kevin Willer, who is the co-founder of the Google Chicago office and is currently a partner at Chicago Ventures, explored the idea of urban planning and the smart city. He advocated the idea of how increase in surveillance threatens to upset the balance of power between city governments and city residents. "Cleaver cities may not necessarily be better ones," he says, since they are not only vulnerable to digital hacks, but are also subject to hacks on the privacy of a citizen. The systems should thus be developed without becoming systems of mass surveillance and promote privacy both by law and the underlying technology infrastructure. He promoted solutions like data factorization, de-identification and transparency.

Richard Warner, who is a professor of law at Kent College, advocated that there should be a clear tradeoff between privacy and security. That is, if citizens we are giving up our data and are continuously monitored by the state, we are doing this bearing in mind that by doing so we are increasing our security. That is to say that since the government is able to monitor our actions, we are more secure now. However, by increasing the amount of data that can be monitored, the problem we are trying to solve becomes that of finding a needle in a haystack. He draws a comparison between the physical ecosystem and a digital one. In a physical ecosystem, we know where the doors are and we can place guards on those doors in order to protect ourselves. This type of effort is futile in a digital ecosystem where we don't know where all the doors are and the guards in place are too easy to fool. He further promoted the idea that surveillance should try to reduce blame on law by increasing cultural surveillance first. He spoke about cyber insurance as an increasingly popular field of study and the sustainability of its commercial model. He concluded by stating that we should individually build up our security and focus on making our computer harder to get to than the other person.

David Thaw, who is an assistant professor of law and information sciences at University of Pittsburg, stated that security and privacy aren't the core competency of a smart city. However, we can thrive to achieve these goals. He advocated that governments should focus their cybersecurity efforts from a standpoint of prevention and not just protection. According to his research, quantitative data collected show that Chief Information Officers in organizations would greatly benefit if they map their risk mitigation techniques to match risk tolerance and risk analysis capabilities. This approach can be utilized to design a digital infrastructure of a smart city.

Ellen Mitchell, who is a professor of psychology at Illinois Institute of Technology, focused her discussion on human behaviors and psychological effects of smart cities. She explained the psychological impact of surveillance and distinguished it from the term monitoring. Monitoring involves an assumption that somebody somewhere is doing something wrong, this assumption is not valid during surveillance. Further, surveillance is not equal for all since employees at the lower level of an organization will be surveyed more than those at higher levels who exhibit legitimate positional power. Though smart cities focus on routine surveillance, we should be mindful of the cost associated with capturing the data and the psychological implication of such surveillance. She promoted the idea of using less technology when you can and promoting a more focused approach to surveillance rather than mass surveillance.

The conference overall was able to bring a plethora of ideas related to privacy and the smart city. These ideas covered domains like law, technology, psychology and sociocultural influences. As individuals we must not only be aware of how we are being monitored but we must ask important questions like, why are we being monitored? What data is being monitored? How secure is our data? There was open discussion of some of the key concepts with the audience. The event was followed by a warm reception where people continued to discuss the things they learnt from the conference. The conference had thus succeeded in leaving an everlasting impression on everyone.