Smart Environments & The Convergence of the Veillances

Privacy violations to consider

Christine Perakslis
College of Management, MBA Graduate Program
Johnson & Wales University
Providence, RI
cperakslis@jwu.edu

Katina Michael
International School of Information Systems and Technology
University of Wollongong
NSW, Australia
katina@uow.edu.au

M.G. Michael
International School of Information Systems & Technology
University of Wollongong
NSW, Australia
mgmichael@uow.edu.au

Abstract— **As a vast array of embedded smart devices will connect to the IoT (Internet of Things), society is rapidly moving into the unchartered territory of Pervasive Technology. Networks of devices will be unobtrusive; thereby freeing humans from the effort of human-to-machine (H2M) interactions, as well as elements of everyday decision-making. Technology will be far more intelligent and ubiquitous, thinking and acting for us behind the lines of visibility. The purpose of this paper is to probe the attributes of pervasive technologies (e.g. smart environments) within the context of the rapidly converging four veillances (i.e. surveillance, dataveillance, sousveillance, and uberveillance), so as to critically identify potential risk events of these processes. The authors utilized a philosophical research approach with intellectual analysis taking into account a framework of privacy border crossings violations for humans so as to yield value judgments and thereby generate discussion in the technology community.**

Keywords- pervasive technology, privacy, smart environments, uberveillance, veillances

I. INTRODUCTION

The authors of this presentation propose risk events and consequences influencing the sociocultural realm when considering the rapidly changing landscape of emerging pervasive technologies. Through the use of a broad and generic, yet internationally recognized, risk assessment framework (ISO 31000:2009), the authors defined the risk category as emerging pervasive technologies (e.g. IoT) and the cause of risk as the converging of the veillances. Using a philosophical research approach with intellectual analysis, the authors adjusted and expanded risk events from previous research [1]. In conclusion, the authors present privacy border violations. In closing, we invite dialogue to ensure robust review in the risk identification process.

II. RISK CATEGORY: PERVASIVE TECHNOLOGY

Society is rapidly entering the unchartered and precarious terrain of an interconnected world of pervasive technology. Machines will continue to be far more intelligent and ubiquitous, thinking and acting for us behind the lines of visibility. An amalgamation of networks of devices will be unobtrusive. Humans will be increasingly freed from the effort of human-to-machine (H2M) interactions. Machines will act autonomously and make decisions for the human [1].

III. RISK CAUSE: THE CONVERGING VEILLANCES

As depicted in Figure 1, the interconnection and reach of the veillances is extensive, and especially in the context of emerging pervasive environments (e.g. smart environments). Veillance, watching or being watched, now extends from the sky (surveillance) to the street (dataveillance) to the person around you (sousveillance) to within you (überveillance) and then ripples out and back to the sky. Physical distance from the human is denoted. The circles have been adapted from previous iterations to appear with dotted lines, representing more permeable boundaries relative to the interrelationships between the veillances. The four veillances are as follows.

A. *Surveillance (e.g. satellite view)*

Surveillance was first recognized in the early 19th century from the French sur meaning “over” and veiller meaning “watch”. This is the veillance of authority; the powerful monitoring the less powerful. Examples include satellites, municipal cameras in streetlights or on/within buildings, or the interception of data for intelligence gathering by a government.

B. *Dataveillance (e.g. street view)*

Dataveillance is the methodical and organized collection or use of digital personal data in the investigation or monitoring of one or more persons [2]. This veillance extends from a veillance of authority to also one of non-authority. Examples include systematic digital monitoring of people as they use the internet, or commercial data mining practices by a company with advanced capabilities in analytics to understand consumer behavior.

C. *Sousveillance (e.g. person view)*

Sousveillance [3] is the capturing of activities from the perspective of one participant in a shared activity with other participants. This is a veillance happening from the person view to other people in the vicinity. Examples include a lifelogger capturing images of others attending an event, or peer-to-peer social media in which your posts are viewed.

D. *Überveillance (e.g. sensor view)*

Überveillance [4] is electronic surveillance within the human body. Some contend it is analogous to big brother on the inside looking out. This veillance has to do with the watching of the fundamental who (ID), where (location), and when (time) of the human. There is the potential for deriving the why (motivation), the what (result), and the how (methods/thoughts) of the human [4]. Examples include medical and non-medical implants (e.g. contact lens "glass" with internet access or iPlants within the human body), or wearables collecting health and sleep data (e.g. heartrate, perspiration, pulse, activity, and temperature).

E. *The Convergence Intensifies*

With pervasive technologies, the veillances are rapidly converging. Information exchanges can now move seamlessly and automatically in and through the human, and out across multiple platforms in each of the veillances. With pervasive technologies, we have more interoperable veillance networks that connect buildings to vehicles to other vehicles to wearables to spatio-temporal tracking bearables, to biosensor data from inside us and back out to be analyzed through advanced algorithms. Pervasive technologies create the methodology for the intensification of convergence.

Überveillance is positioned central because it can uniquely bring together all forms of watching from above, below, beside, and from within by involuntarily or voluntarily using obtrusive or unobtrusive devices. As pervasive environments develop, internal data gleaned from the human can be ever more combined and synthesized with data from across the spectrum of veillances. The consequence is rich, broad, deep, sensitive, and highly private personal data mining. The data can be analyzed relative to the current physiological and/or psychological state; predictive analytics can increasingly forecast the future state of the human.

IV. Risks events in synthesized environments

When synthesizing the environments of pervasive technology (risk category) and the converging veillances (risk cause), we propose six risks (risk events), as follows.

A. *Insightfulness*

With context-awareness and context-adaption, ubiquitous devices will be continuously "on" and autonomously learning behaviors. With data gleaned across all veillances, devices will assess humans in multiple contexts, capacities, and over time. This is likely to lead to a capability for the system to have rich insightfulness, or a precise and profound understanding of humans in the current, but also future, state.

B. *Imperceptible*

As networks are operating behind the line of visibility, humans are not likely to comprehend the scope, or reach, or even timing of data practices. The processes and procedures are likely to be imperceptible. Users could be blinded to what is collected, by whom, for how long, how it is synthesized with other data, and who owns the data.

C. *Incomprehensibility*

Terms and conditions are often murky and/or mutable. Additionally, the average human is not likely to comprehend the wide-ranging system, nor the risks associated across multiple organizations sharing data. The system is likely to be incomprehensible for the consumer. Simpler technologies have already proven to be complex and convoluted to the average consumer.

D. *Indelibility*

Data may become ineradicable – somewhere within the veillances. Our digital footprints are likely to leave an indelible history of analyzable behaviors, especially if we do not own our data, or if data were shared and stored elsewhere in the veillances.

E. *Invasiveness*

As we allow devices to listen inside of us and communicate back and forth between the veillances, we are likely to create systems in which not only our behaviors are predicted, but even our intent. Dignity could be at risk – even if unintended.

F. *Involuntariness*

Opting-in to technology is becoming a requirement to participate in society. It is evermore compulsory for an individual to subscribe to cloud-based email to be gainfully employed or to receive extensive services across disciplines at a hospital. More often, individuals are pressured to opt-in to belong and benefit socially, or to benefit financially (e.g. discounts offered by an insurance company).

V. Conclusion: Socio-cultural consequences to consider

When considering the risk events, the authors suggest there are likely to be socio-cultural consequences relative to autonomy and privacy.

A. *Autonomy: Participation in Society*

With greater pressure on individuals to opt-in to participate in society, and less control over processes and ownership of our personal data, we may be increasingly forced into tolerating these risks. Examples may include opting-in to wearables that collect biosensor data to receive

ISBN: 978-1-61208-4763

lower insurance premiums, or agreeing to cloud-based storage of sensitive data to remain gainfully employed.

B. Privacy: Probably Border Violations

To mine out privacy issues, the authors chose to examine the four borders of privacy as defined by Marx [5], a leading figure in surveillances studies. Marx proposed four borders as follows. Natural Borders are privacy boundaries relative to such elements as those that are materially observable such as walls, doors, clothing, facial expressions, and verbal conversations. Social Borders are privacy boundaries relative an individual's expectations such as confidentiality with professionals or family/friends, freedom from invasion of privacy by others in the social system. Spatial or Temporal Borders are privacy boundaries relative to an individual's expectations such as the right to establish delineation between various areas of an individual's life (work, personal, religious spheres) or at various points in time; rights to maintain decoupled spheres. Borders due to Ephemeral or Transitory Effects are privacy boundaries relative to an individual's expectations such as the right to have information forgotten, or to delete permanently a past extemporaneous or regrettable action [5].

When weighing the aforementioned proposed risks (events) against the four borders of privacy to yield consequences, we concluded that pervasive technologies are likely to violate all four privacy borders in the current societal context.

VI. DISCUSSION

In closing, we invite consultation relative to the risks identified and the conclusions presented so as to purposefully anticipate the risk events leading to socio-cultural impacts of pervasive technology fueling veillance capability. We do not want to unnecessarily obstruct progress to commercialize products. We contend that a collaborative risk identification process will allow for a more robust anticipatory approach to ensure that sociocultural issues are identified well and earlier in the process. Perhaps this will stimulate efforts to apply approaches such as Anticipatory Ethics, Privacy by Design (PbD), and/or the International Associations of Impact Assessments' (IAIA) Social Impact Assessment (SIA)/Privacy Impact Assessment (PIA).

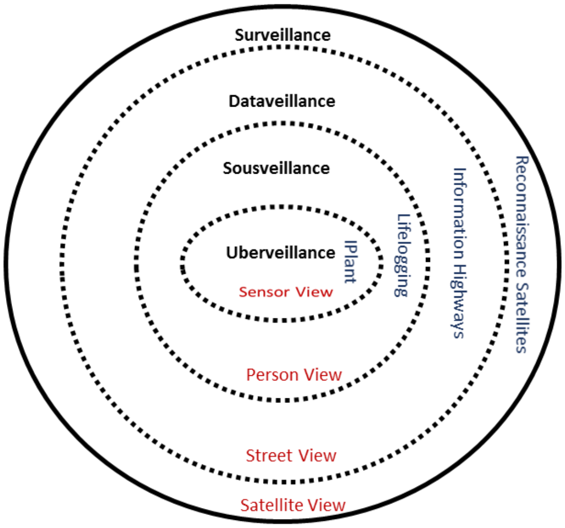

Figure 1 The Veillances Original diagram Michael, Michael, & Abbas, 2009; Adapted by Michael, Michael, & Perakslis, 2013

REFERENCES

[1] Perakslis, C, Michael K, Michael, M. Pervasive Technologies: Principles to consider. Ethics in Biology, Engineering and Medicine: An international journal. 2014; 5(1): 79-93.

[2] Clarke R. Just another piece of plastic in your wallet: the `Australian card' scheme. ACM SIGCAS Computers and Society. 1988b;18:7-21.

[3] Mann S, Nolan J, Wellman B. Sousveillance: Inventing and Using Wearable Computing Devices for Data Collection in Surveillance Environments. Surveillance and Society. 2003;1:331-55.

[4] Michael K, Michael MG. From Dataveillance to Überveillance and the Realpolitik of the Transparent Society. The Social Implications of National Security. Wollongong, NSW, Australia2007a.

[5] Marx, G. Murky Conceptual Waters: the Public and the Private in Ethics and Information Technology, 2001; 3: 157-169.