

'Smart Cities' Are the Next Phase in the 21st Century Surveillance Grid

By Steven MacMillan

Global Research, June 16, 2015

New Eastern Outlook 15 June 2015

Region: <u>USA</u> Theme: <u>Intelligence</u>

The century of 'big data' will be the century of unprecedented surveillance. The dream of tyrants down through history has been the total monitoring, control and management of the public, with the ability to predict the behaviour of entire populations the most efficient means of achieving this objective. For millennia, this has mainly existed in the realm of fantasy, however with the vast leap in technology in recent decades, this idea is becoming less a dystopian science fiction movie and more the daily business of totalitarian high-tech regimes.

Most readers are now familiar with the predatory surveillance practices of agencies such as the NSA and GCHQ, which high-level NSA whistleblower William Binney describes as "totalitarian" in nature, adding that the goal of the NSA is "to set up the way and means to <u>control the population</u>". Yet many people may not be aware of the next phase in 21st century surveillance grid; the 'smarter city'.

Promoted by some as a low-cost and efficient way of managing the workings of a city, others see the surveillance implications of such initiatives as chilling to say the least. Smart cities are broadly defined as digitally connected urban areas filled with ubiquitous sensors, monitors and meters, which collect data on every aspect of the city; from energy usage, to transport patterns. This data is then analysed and used by city planners to 'improve decision making'.

Today, more than <u>half the world's population</u> lives in urban areas – a trend that is set to accelerate into the future – meaning the smart city concept is going to affect the lives of billions of people around the world. India is at the forefront of this push as it plans to build <u>100 smart cities</u> in the coming years, with Singapore set to become the <u>world's first smart nation</u>. Smart cities are not just confined to Asia however, as Glasgow (where I'm writing from), Rio de Janeiro, New Orleans and Cape Town are just a handful of cities involved in IBM's "smarter cities challenge".

Privacy in a Smart City

The global move towards a 'smarter planet' is a worrying prospect for many who are concerned with the growing erosion of privacy in the modern world. Can privacy exist in a smart city where every corner and crevice of the urban environment is fitted with digital sensors collecting data on every movement of the city 24 hours a day?

Furthermore, many of the supporters and proponents of smart initiatives are multinational corporations and notorious foundations, including IBM, Siemens, Cisco and the Rockefeller Foundation. The notion of corporate giants managing a smarter planet becomes even more

troubling when you consider the history of companies such as IBM, which played a pivotal role in the holocaust and worked closely with <u>Nazi Germany</u>. Given IBM's dark history, should we trust it with the power to regulate and manage numerous cities around the world?

In an article for <u>AlterNet</u> titled: <u>The Terrifying "Smart" City of the Future</u>, <u>Allegra Kirkland</u> details some of the more disturbing aspects of a smarter planet:

"The surveillance implications of these sorts of mass data-generating civic projects are unnerving, to say the least. Urban designer and author Adam Greenfield wrote on his blog Speedbird that this centralized governing model is "disturbingly consonant with the exercise of authoritarianism." To further complicate matters, the vast majority of smart-city technology is designed by IT-systems giants like IBM and Siemens. In places like Songdo, which was the brainchild of Cisco Systems, corporate entities become responsible for designing and maintaining the basic functions of urban life.... Private corporations are the ones measuring and controlling these mountains of data, and that they don't have the same accountability to the public that government does."

The Age of Big Data and Predictive Policing

The amount of data generated in recent years has skyrocketed, with IBM CEO Ginni Rometty noting in a 2013 speech that "90% of all the data ever known to man has been created in the last two years". With this trend only set to continue into the future, the race is now on to develop systems to accurately predict the behaviour of entire populations through scanning copious volumes of data for behavioural patterns.

In Australia, the federal crime commission is now using big data systems to analyse patterns of behaviour in a quest to <u>predict criminal activities</u> before they occur. It seems the world is moving closer to the themes in the 1950's science fiction story by Philip K. Dick and the later film adaptation of the work, 'The Minority Report'.

It is not just Australia however that is engaged in such activities, as the Los Angeles Police Department (LAPD) has a division called the <u>Real-Time Analysis and Critical Response Division</u> (RACR). The RACR uses cutting-edge algorithmic systems and analytics in an attempt to predict future crime. British police in Kent have also been using a precrime software program called <u>Predpol</u> for two years, which analyses crimes based on date, place and category of offence, in order to assist police in making decisions on patrol routes.

The ethical and moral questions of the move towards predictive policing are obvious, leading many to fear a potential 'tyranny of the algorithm' in the future. With big data being used in the field of law enforcement to *surveil* and attempt to predict criminal behaviour, you can be assured that intelligence agencies and corporations will be using big data in the futuristic smart city to monitor and predict the behaviour of the city's population.

Crystal Ball Software

Back in 2010, we got a glimpse into the intentions of the <u>CIA and Google</u> when they funded a start-up company called 'Recorded Future', an organisation that claimed to have technology that could predict the future through collecting data from the internet. 'Recorded Future' attempts to scan the entire web looking for patterns and analyzing

information on a global scale; with the companies CEO <u>Christopher Ahlberg</u> revealing that the software scans "8 billion data points, [from] 600, 000 sources" each week.

As the Internet of Things (IoT) continues to expand in size and scope producing even more data, demand for companies such as 'Recorded Future' by intelligence agencies and corporations will continue to increase. <u>Techopedia</u> defines the IoT as a "computing concept that describes a future where everyday physical objects will be connected to the Internet and be able to identify themselves to other devices." The number of devices connected to the internet has exploded in recent years, a trend that Cisco details in a 2011 report:

"In 2003, there were approximately 6.3 billion people living on the planet and 500 million devices connected to the Internet... Explosive growth of smartphones and tablet PCs brought the number of devices connected to the Internet to 12.5 billion in 2010... Cisco IBSG predicts there will be 25 billion devices connected to the Internet by 2015 and 50 billion by 2020."

Many have voiced privacy concerns over the idea of the internet being embedded in everything considering the fact that government agencies and corporate entities have been illegally collecting vast swaths of personnel information from the internet for years. As <u>Michael Snyder</u> writes in a recent article, "could an IoT create a dystopian nightmare where everyone and everything will be constantly monitored and tracked by the government?"

We are truly entering a 'Brave New World', where science fiction is becoming reality. But what input will the people of the world have in the creation of this 'Brave New World', and what role will representative government play?

Steven MacMillan is an independent writer, researcher, geopolitical analyst and editor of <u>The Analyst Report</u>, especially for the online magazine <u>"New Eastern Outlook"</u>.

The original source of this article is <u>New Eastern Outlook</u> Copyright © <u>Steven MacMillan</u>, <u>New Eastern Outlook</u>, 2015

Comment on Global Research Articles on our Facebook page

Become a Member of Global Research

Articles by: Steven MacMillan

Disclaimer: The contents of this article are of sole responsibility of the author(s). The Centre for Research on Globalization will not be responsible for any inaccurate or incorrect statement in this article. The Centre of Research on Globalization grants permission to cross-post Global Research articles on community internet sites as long the source and copyright are acknowledged together with a hyperlink to the original Global Research article. For publication of Global Research articles in print or other forms including commercial internet sites, contact: publications@globalresearch.ca

www.globalresearch.ca contains copyrighted material the use of which has not always been specifically authorized by the copyright owner. We are making such material available to our readers under the provisions of "fair use" in an effort to advance a better understanding of political, economic and social issues. The material on this site is distributed without profit to those who have expressed a prior interest in receiving it for research and educational purposes. If you wish to use copyrighted

material for purposes other than "fair use" you must request permission from the copyright owner.

For media inquiries: publications@globalresearch.ca