Surveillance Society

Introduction

Assume that you have been appointed to a task force of 5 or 6 computing professionals within your organization. You have been asked to examine the current issue outlined in the article below. Your team has not been asked to make specific recommendations to solve the problem. Rather, you have been asked to make recommendations that will help the Government decide what next steps they should take.

Prompts

1. What is/are the problem/problems here? Is there an underlying fundamental problem?
2. Who are the major stakeholders and what are their perspectives?
3. What are the major ethical, legal, and security aspects associated with the problem?
4. What are the intended and unintended consequences of existing computing solutions? Consider the consequences on individuals, organizations and society within local and global contexts.
5. What recommendations do you propose that may lead to potential solutions?

How private are our lives? What information can be found out about our interests, friends and activities? Data is collected from closed-circuit television (CCTV) cameras placed on the streets, in the workplace, schools and malls. Our phones send information about our location and movements, speed cameras track the speed and location of our cars, the Internet records which sites we visit, what we buy, social networking sites know our interests and activities, family and friends. Smart TVs know what we're watching and companies record and analyse what we buy. Apps record when we are awake and sleep, and how much exercise we've done during the day. Add to that bank of data our phone records, email addresses, downloads, medical records, shopping receipts, bank balances, travel itineraries and credit card information. How much privacy do we have?

In the past limited information could be stored and analysed but now mass data can be collected, stored and analysed by government agencies and private companies. For example, the UAE government spent $1 billion in 2015 on surveillance solutions and in Dubai the police made the installation of CCTV in 25000 residential and commercial buildings compulsory. Our activities generate metadata, which is data about data. For example, when we send a text we generate metadata about our location, type of phone, time of text, how many bits in text, the carrier used, the time the text was made and received, information about the recipient, and so on. Web

hosts, social media and telecommunication companies collect our digital trail. Metadata is not subject to the same privacy restrictions as the contents of a message, and there is debate over the distinction between data and metadata. Using higher encryption can protect metadata, and masking IP addresses by using Virtual Private Networks (VPNs), but these can be illegal in the UAE, dependent on what they are used for.

Collecting data is not surveillance until it is analysed. Collecting and storing information is cheaper than analyzing it, although better analytical software is being developed. Through mass surveillance and trawling, metadata can be analysed to create extremely detailed profiles. As 96% of Google's revenue comes from advertising, this information is valuable. It is also valuable to government programs such as Prism; huge intelligence dragnets that apply algorithms to big data.

Internet users trade privacy for benefits, such as Google tracking our Internet searches so it can show relevant advertisements. People post personal photos on social media, share credit card information to strangers, enter personal information to sign up to sites. Users want privacy but also the convenience of their technological devices being personalized and knowing their preferences.

A popular way of gathering data is CCTV, and surveillance footage from CCTV has been an important tool in solving crimes. There is a growing trend of putting surveillance cameras in homes in the Gulf to watch maids. In Ras Al Khaimah, a maid was caught beating a child on CCTV, and a Saudi family caught their maid urinating on their food. While maids say they don't like to be watched, some claim the employer has the right to watch an employee's activities and the line between surveillance and breach of privacy remains unclear. Government officials installed CCTV in a customer service centre in the UAE and were convicted of breaching employee privacy, and given jail terms. However, cultural issues may be a factor in this case as the service centre was for female customers.

CCTV on the streets has also been a useful tool for the police to catch criminals and make roads safer. When bombs detonated at the Boston Marathon, the people responsible were caught from surveillance camera footage. Recently in the UAE, pedestrians were killed in hit and run accidents and police were able to catch the drivers with the images recorded on CCTV as evidence. By 2011, 25000 CCTV

cameras had been installed in Dubai, covering approximately 90% of public areas. “There is no point in fleeing the scene of a crime or accident as there is an extensive smart surveillance system in place to monitor the roads,” the Head of Abu Dhabi Police Traffic claims.

In America, public opinion is divided over this issue. According to the Pew research Centre, 56% of Americans think the government getting court orders to track the phone records of millions of Americans is acceptable. Many people think intrusions on their privacy are acceptable if it informs the government about terrorist threats. Interestingly, younger Americans are more opposed to their privacy being invaded, even if it keeps them safer from terrorism.

Governments assure us that they won’t search the metadata they have access to unless they have a reason, such as terrorism. However surveys show that many of the public believe the government is listening to their phone calls and reading their emails. In many countries, such as America, there are measures in place to protect the privacy of Americans, but is this the case in other countries? In America there are regulations about the way the government can search data. For example, only specially trained analysts can search the databases in a specific way if they are suspicious about a particular phone number. They can then only use this information in a limited way, to map other numbers to that number.

It is clear there is a balance between surveillance to keep the public safe, respecting privacy and following regulations in countries such as the UAE. There is now more surveillance because the amount of data that is collected and analysed is increasing. There is secrecy around surveillance programs, and so we don’t know how much privacy we actually have. Information is power, and the government has the authority to act on information, such as prosecuting and imprisoning us.

Bibliography

Al Ghalib, E. (2011, July 13). *Police make four arrests using surveillance cameras.* Retrieved April 21, 2016, from The National : http://www.thenational.ae/news/uae-news/police-make-four-arrests-using-surveillance-cameras

Dajani, H. (2015, April 29). *Abu Dhabi government officials cleared of breaching staff privacy.* Retrieved April 21, 2016, from The National :

http://www.thenational.ae/uae/courts/20150429/abu-dhabi-government-officials-cleared-of-breaching-staff-privacy

Drehle, D. V. (2013, August 1). *The Surveillance Society* . Retrieved April 21, 2016, from TIME: http://nation.time.com/2013/08/01/the-surveillance-society/

Its better to trust staff than spy on them . (2013, May 3). Retrieved April 21, 2016, from The National : http://www.thenational.ae/opinion/editorial/its-better-to-trust-staff-than-spy-on-them

Majority Views NSA Phone Tracking as Acceptable Anti-terror Tactic. (2013, June 10). Retrieved April 21, 2016, from PEW Research Centre : http://www.people-press.org/2013/06/10/majority-views-nsa-phone-tracking-as-acceptable-anti-terror-tactic/

Miles, G. (2013, August 1). *Americans Sharply Split on Privacy Issues.* Retrieved April 21, 2016, from TIME: http://nation.time.com/2013/08/01/americans-sharply-split-on-privacy-issues/

Smart Surveillance in the GCC: Key trends and outlook. (2014). Retrieved April 21, 2016, from MEED Insight: http://www.meed.com/Journals/2014/09/08/h/d/l/MEED-Insight-Surveillance-Research-paper-WEB.pdf