TERM PAPER ON

ETHICAL CHALLENGES AND ISSUES ON THE USE OF SURVEILLANCE TECHNOLGY

BY

GROUP 13

PROFESSIONAL AND SOCIAL ASPECTS OF COMPUTING

(COSC 409)

DEPARTMENT OF MATHEMATICS

AHMADU BELLO UNIVERSITY, ZARIA

GROUP 13 MEMBERS

NAMES	REG NO	SIGN
SADIQ KHALIL ABUBAKAR	**U12CS2019**	_____
MOHAMMED HAMISU ISAH	**U11CS2046**	_____
HARUNA ABDULLAHI KAWO	**U12CS2022**	_____
HARUNA YUSUF MURTALA	**U12CS2028**	_____
AUWAL YAHAYA	**U12CS2023**	_____
UMAR ADAM	**U12CS2018**	_____
ABBAS ADAMU ABUBAKAR	**U12CS2016**	_____
EPHRAIM YUSUF	**U12CS2020**	_____
MUSTAPHA ABDULKADIR SANI	**U13CS3004**	_____
KELANI JELILAT TOSIN	**U12CS2014**	_____
RAHINA MUSA	**U12CS2015**	_____
KHADIJA ILYASU	**U12CS2017**	_____
MARYAM IDRIS	**U12CS2025**	_____
MARYAM DAHIRU	**U12CS2029**	_____

Abstract

This paper focuses on ethical challenges and issues on the use of surveillance technologies. Surveillance comes from the French word ‘surveiller’ which means to watch from above, is the monitoring of the behavior, activities, or other changing information, usually of people for the purpose of influencing, managing, directing, or protecting them. The government defines a surveillance operation as an event during which the activities of a particular individual or group are observed and documented.

Surveillance is used by government for intelligence gathering, the prevention of crime, the protection of a process, person, group or object, or for the investigation of crime. It is also used by criminal organizations to plan and commit crimes such as robbery and kidnapping, by businesses to gather intelligence, and by private investigators.

Surveillance is often a violation of privacy, and is opposed by various civil liberties groups and activists. Liberal democracies have laws which restrict domestic government and private use of surveillance, usually limiting it to circumstances where public safety is at risk. Authoritarian governments rarely have any domestic restrictions; and international espionage is common among all types of countries.

There could be other ethical challenges on the use of surveillance technologies, but this paper only poses a few of these ethical challenges which are invasion of privacy, psychological/social effects and totalitariansm.

1. Introduction

The term surveillance encompasses not only visual observation but also the scrutiny of all behavior, speech, and actions. Prominent examples of surveillance include surveillance cameras, wiretaps, GPS tracking, internet surveillance and a host of others. One-way observation is in some way an expression of control. Just as having a stranger stare at you for an extended period of time can be uncomfortable and hostile; it is no different from being under constant surveillance, except that surveillance is often done surreptitiously and at the behest of some authority.

Oppositions to surveillance started by individuals like Jeremy Bentham, whose idea of the Panopticon is arguably the first significant reference to surveillance ethics in the modern period, after him came George Orwell who extended the Panopticon to encompass the whole of society, or at least the middle classes and Michel Foucault who again extended George Orwell's novel titled 1984, in this novel the Panopticon became electrical with the invention of the telescreen, a two-way television which allowed the state almost total visual and auditory access to the homes, streets and workplaces of the citizens. Foucault's particular concern was with the use of power and its increasing bureaucratization in the modern period. His study began with torture and the emphasis on the sovereignty and power of the king. With the Enlightenment the prison was introduced as a more efficient means of punishment, supported by society's increasing acceptance of the value of discipline beyond merely the military or religious arenas.

Today's technological capabilities take surveillance to new levels; no longer are spyglasses and "dropping" from the eaves of a roof necessary to observe individuals, the government can and does utilize methods to observe all the behavior and actions of people without the need for a spy to be physically present. Clearly, these advances in technology have a profound impact with regards to the ethics of placing individual under surveillance, in our modern society, where so many of our actions are observable, recorded, searchable, and traceable, close surveillance is much more intrusive than it has been in the past.

The rest of the paper is organized as follows; section 2.1 focuses on surveillance technologies, section 3.1 on ethical challenges of surveillance technologies, section 4.1 is spotlight's issues on the use of surveillance technologies and 5.1 concludes the paper.

2.1 Surveillance technologies

Surveillance technologies are tools used for implementing surveillance, there are a whole lot of these technologies out there, but this paper will pose the major types of surveillance technologies:

Computer

The vast majority of computer surveillance involves the monitoring of data and traffic on the Internet. In the United States for example, under the Communications Assistance For Law Enforcement Act, all phone calls and broadband Internet traffic (emails, web traffic, instant messaging, etc.) are required to be available for unimpeded real-time monitoring by Federal law enforcement agencies. There is far too much data on the Internet for human investigators to manually search through all of it. So automated Internet surveillance computers sift through the vast amount of intercepted Internet traffic and identify and report to human investigators traffic considered interesting by using certain "trigger" words or phrases, visiting certain types of web sites, or communicating via email or chat with suspicious individuals or groups. Billions of dollars per year are spent, by agencies such as the Information Awareness Office, NSA, and the FBI, to develop, purchase, implement, and operate systems such as Carnivore, NarusInsight, and ECHELON to intercept and analyze all of this data, and extract only the information which is useful to law enforcement and intelligence agencies.

Telephones

The official and unofficial tapping of telephone lines is widespread. In the United States for instance, the Communications Assistance for Law Enforcement Act (CALEA) requires that all telephone and VoIP communications be available for real-time wiretapping by Federal law enforcement and intelligence agencies. Two major telecommunications companies in the U.S AT&T Inc. and Verizon, have contracts with the FBI, requiring them to keep their phone call records easily searchable and accessible for Federal agencies, in return for $1.8 million per year. Between 2003 and 2005, the FBI sent out more than 140,000 "National Security Letters" ordering phone companies to hand over information about their customers' calling and Internet histories. About half of these letters requested information on U.S. citizens. Human agents are not required to monitor most calls. Speech-to-text software creates machine-readable text from intercepted audio, which is then processed by automated call-analysis programs, such as those developed by agencies such as the Information Awareness Office, or companies such as Verint, and Narus, which search for certain words or phrases, to decide whether to dedicate a human agent to the call. Law enforcement and intelligence services in the United Kingdom and the United States possess technology to activate the microphones in cell phones remotely, by accessing phones' diagnostic or maintenance features in order to listen to conversations that take place near the person who holds the phone.

Cameras

Surveillance cameras are video cameras used for the purpose of observing an area. They are often connected to a recording device or IP network, and may be watched by a security guard or law enforcement officer. Cameras and recording equipment use to require human personnel to monitor camera footage, but analysis of footage has been made easier by automated software that organizes digital video footage into a searchable database, and by video analysis software (such as VIRAT and HumanID). The amount of footage is also drastically reduced by motion sensors which only record when motion is detected.

Governments often initially claim that cameras are meant to be used for traffic control, but many of them end up using them for general surveillance. For example, Washington, D.C. had 5,000 "traffic" cameras installed under its premise, and then after they were all in place, networked them all together and then granted access to the Metropolitan Police Department, so they could perform "day-to-day monitoring". The development of centralized networks of CCTV cameras watching public areas, linked to computer databases of people's pictures and identity (biometric data), able to track people's movements throughout the city, and identify whom they have been with; has been argued by some to present a risk to civil liberties. Trapwire is an example of such a network.

Social network analysis

One common form of surveillance is to create maps of social networks based on data from social networking sites such as Facebook, MySpace, and Twitter as well as from traffic analysis information from phone call records such as those in the NSA call database, and others. These social network "maps" are then data mined to extract useful information such as personal interests, friendships & affiliations, wants, beliefs, thoughts, and activities. Many U.S. government agencies such as the Defense Advanced Research Projects Agency (DARPA), the National Security Agency (NSA), and the Department of Homeland Security (DHS) are investing heavily in research involving social network analysis.

AT&T developed a programming language called "Hancock", which is able to sift through enormous databases of phone call and Internet traffic records, such as the NSA call database, and extract "communities of interest", groups of people who call each other regularly, or groups that regularly visit certain sites on the Internet. AT&T originally built the system to develop "marketing leads", but the FBI has regularly requested such information from phone companies such as AT&T without a warrant, and after using the data stores all information received in its own databases, regardless of whether or not the information was ever useful in an investigation.

Some people believe that the use of social networking sites is a form of "participatory surveillance", where users of these sites are essentially performing surveillance on themselves, putting detailed personal information on public websites where it can be viewed by corporations and governments. In 2008, about 20% of employers reported using social networking sites to collect personal data on prospective or current employees.

Biometric

Biometric surveillance is any technology that measures and analyzes human physical and/or behavioral characteristics for authentication, identification, or screening purposes. Examples of physical characteristics include fingerprints, DNA, and facial patterns. Examples of mostly behavioral characteristics include gait (a person's manner of walking) or voice. Facial recognition is the use of the unique configuration of a person's facial features to accurately identify them, usually from surveillance video. Both the Department of Homeland Security and DARPA are heavily funding research into facial recognition systems. The Information Processing Technology Office ran a program known as Human Identification at a Distance which developed technologies that are capable of identifying a person at up to 500 ft by their facial features. Another form of behavioral biometrics, based on affective computing, involves computers recognizing a person's emotional state based on an analysis of their facial expressions, how fast they are talking, the tone and pitch of their voice, their posture, and other behavioral traits. This might be used for instance to see if a person is acting "suspicious" (looking around furtively, "tense" or "angry" facial expressions, waving arms etc.). A more recent development is DNA profiling, which looks at some of the major markers in the body's DNA to produce a match. The FBI is spending $1 billion to build a new biometric database, which will store DNA, facial recognition data, iris/retina (eye) data, fingerprints, palm prints, and other biometric data of people living in the United States. The computers running the database are contained in an underground facility about the size of two American football fields. Facial thermographs are in development, which allow machines to identify certain emotions in people such as fear or stress, by measuring the temperature generated by blood flow to different parts of their face. Law enforcement officers believe that this has potential for them to identify when a suspect is nervous, which might indicate that they are hiding something, lying, or worried about something.

RFID and Geolocation Devices

Radio Frequency Identification (RFID) tagging is the use of very small electronic devices (called "RFID tags") which are applied to or incorporated into a product, animal, or person for the purpose of identification and tracking using radio waves. The tags can be read from several meters away. They are extremely inexpensive, costing a few cents per piece, so they can be inserted into many types of everyday products without significantly increasing the price, and can be used to track and identify these objects for a variety of purposes. Some companies appear to be "tagging" their workers by incorporating RFID tags in employee ID badges. Workers in U.K. considered strike action in protest of having themselves tagged; they felt that it was dehumanizing to have all of their movements tracked with RFID chips. Some critics have expressed fears that people will soon be tracked and scanned everywhere they go. On the other hand, RFID tags in newborn baby ID bracelets put on by hospitals have foiled kidnappings. Verichip is an RFID device produced by a company called Applied Digital Solutions (ADS). Verichip is slightly larger than a grain of rice, and is injected under the skin. The injection reportedly feels similar to receiving a shot. The chip is encased in glass, and stores a "VeriChip

Subscriber Number" which the scanner uses to access their personal information, via the Internet, from Verichip Inc.'s database, the "Global VeriChip Subscriber Registry". Thousands of people have already had them inserted. In Mexico, for example, 160 workers at the Attorney General's office were required to have the chip injected for identity verification and access control purposes. In a 2003 editorial, CNET News.com's chief political correspondent, Declan McCullagh, speculated that, soon, every object that is purchased, and perhaps ID cards, will have RFID devices in them, which would respond with information about people as they walk past scanners (what type of phone they have, what type of shoes they have on, which books they are carrying, what credit cards or membership cards they have, etc.). This information could be used for identification, tracking, or targeted marketing.

3.1 Ethical challenges of surveillance technologies

"If you haven't done anything wrong, you have nothing to fear." This is a typical argument used by governments and other groups to justify their spying activities. Upon cursory inspection, it seems to make sense as most people are law-abiding citizens, most ostensibly will not be targeted for surveillance and it will not impact their lives, while making their lives more comfortable and safer through the elimination of criminals. Thus, the government's use of closed-circuit television cameras in public spaces, warrantless wiretapping, and library record checks have the potential to save lives from criminals and terrorists with only minimal invasion of its citizens' privacy. First, as a mental exercise, we ask that the reader consider that these arguments could easily be applied to asking all citizens to carry location tracking devices, it would make tracing criminal acts much easier, and that it could easily be argued that people refusing to carry these devices only do so because they have something to hide. It is a matter of course that most people in our society would object to this solution, not because they wish to commit any wrongdoings, but because it is invasive and prone to abuse. Now consider that, given current technology, the government already has the ability to track a known target's movements to a reasonable degree, and has easy access to information such as one's purchasing habits, online activities, phone conversations, and mail. Though implementing mandatory location tracking devices for the whole population is certainly more invasive than the above, we argue that current practices are analogous, extreme, and equally unacceptable.

Next, this argument fails to take into consideration a number of important issues when collecting personally identifiable data or recording; first, that such practices create an archive of information that is vulnerable to abuse by trusted insiders; one example emerged in September 2007, when Benjamin Robinson, a special agent of the Department of Commerce, was indicted for using a government database called the Treasury Enforcement Communications System (TECS) for tracking the travel patterns of an ex-girlfriend and her family. Records show that he used the system illegally at least 163 times before he was caught (Mark 2007). With the expansion of surveillance, such abuses could become more numerous and more egregious as the amount of personal data collected increases.

Invasion of Privacy

One of the core arguments against surveillance is that it poses a threat to privacy, which is of value to the individual and to society. Numerous civil rights groups and privacy groups oppose surveillance as a violation of people's right to privacy. Such groups include: Electronic Privacy Information Center, Electronic Frontier Foundation, and American Civil Liberties Union. Privacy is also of value to society at large. As noted, we may appear in public safe in the knowledge that our weaknesses are not on display for all to see, allowing for confident personal interaction. When we vote we do so in the belief that no-one can see our decision and treat us well or poorly in the light of how we voted. Privacy is thus important in the social context of democracy. In many cases we do not want to know everything about everyone around us and so privacy can protect the rest of us from being exposed to too much information. Thanks to a level of anonymity I may also feel emboldened to speak out publicly against corruption or injustice, or simply to be more creative in self-expression.

Psychological/social effects

Some critics, such as Michel Foucault, believe that in addition to its obvious function of identifying and capturing individuals who are committing undesirable acts, surveillance also functions to create in everyone a feeling of always being watched, so that they become self-policing. This allows the State to control the populace without having to resort to physical force, which is expensive and otherwise problematic. The concept of panopticism is a means of indirect control over a large populous through the uncertainty of surveillance. Michel Foucault analyzed the architecture of the prison panopticon, and realized that its success was not just in its ability to monitor but also its ability to not monitor without anyone knowing. Critics such as Derrick Jensen and George Draffan, argue that panopticism in the United States began in World War I, when the issuing of passports became important for the tracking of citizens and possibly enemies of the state. Such surveillance continues today through government agencies in the form of tracking internet usage and library usage.

Totalitarianism

Totalitarianism is a political system in which the state holds total authority over the society and seeks to control all aspects of public and private life wherever possible.

A person, who is part of a political group which opposes the policies of the national government, might not want the government to know their names and what they have been reading, so that the government cannot easily subvert their organization, arrest, or kill them. Other critics state that while a person might not have anything to hide right now, the government might later implement policies that they do wish to oppose, and that opposition might then be impossible due to mass surveillance enabling the government to identify and remove political threats. Further, other critics point to the fact that most people do have things to hide. For example, if a person is looking for a new job, they might not want their current employer to know this. Also if an employer wishes total privacy to watch over their own employee and secure their financial

information it may become impossible, and they may not wish to hire those under surveillance. The most concern of detriment is securing the lives of those who live under total surveillance willingly, educating the public to those under peaceful watch while identifying terrorist and those who use the same surveillance systems and mechanisms in opposition to peace, against civilians, and to disclose lives removed from the laws of the land.

Programs such as the Total Information Awareness program and laws such as the Communications Assistance for Law Enforcement Act have led many groups to fear that society is moving towards a state of mass surveillance with severely limited personal, social, political freedoms.

Kate Martin, of the Center for National Security Studies said of the use of military spy satellites being used to monitor the activities of U.S. citizens: "They are laying the bricks one at a time for a police state." Some point to the blurring of lines between public and private places, and the privatization of places traditionally seen as public (such as shopping malls and industrial parks) as illustrating the increasing legality of collecting personal information. Traveling through many public places such as government offices is hardly optional for most people, yet consumers have little choice but to submit to companies' surveillance practices. Surveillance techniques are not created equal; among the many biometric identification technologies, for instance, face recognition requires the least cooperation. Unlike automatic fingerprint reading, which requires an individual to press a finger against a machine, this technique is subtle and requires little to no consent.

4.1 Issues on the Use of Surveillance Technology

Surveillance requires infrastructure, staffing, training and maintenance

The hidden costs of infrastructure, training and staffing, operations, and maintenance can dwarf the cost of acquiring surveillance technology in the first place. Communities that have failed to accurately estimate the full financial cost of a surveillance system have dealt with massive cost overruns and programs that fail to accomplish their stated purpose. For example, Philadelphia planned to spend $651,672 for a video surveillance program featuring 216 cameras. Instead, it spent $13.9 million on the project and wound up with only 102 functional cameras after a year, a result the city controller described as “exceedingly alarming, and outright excessive, especially when $13.9 million is equivalent to the cost of putting 200 new police recruits on our streets.” To avoid a similar incident, it is essential to identify all of the costs required to install, use, and maintain surveillance technology before making a decision about whether to do so.

Surveillance can create financial risks including litigation and data breach

Surveillance can carry a number of legal risks. Programs that fail to include proper safeguards for freedom of expression, association, and religion, or that inadequately enforce such safeguards, can lead to expensive litigation. For example, Muslim residents in Orange County filed a discrimination lawsuit when it was revealed that state agents were sending informants into mosques to collect information on the identities and activities of worshippers. Even technical

glitches can create the potential for costly lawsuits and other expenses: the City of San Francisco is still embroiled in a multi-year civil rights lawsuit after wrongly pulling over, handcuffing, and holding at gunpoint an innocent woman due to an error by its ALPR system. The collection of surveillance data also creates the risk of data breach liability. Even following best practices (which itself can entail significant expense) is not enough to prevent every breach. California law now requires that a local agency notify residents about a security breach. And the fiscal costs of a breach of sensitive surveillance data could be very high: a 2012 report found that companies spent an average of $5.5 million to resolve a data security breach. The more information your community collects and retains, the greater the risk and potential cost of a breach.

Funds spent on surveillance may be wasted due to community backslash

Failing to thoroughly discuss surveillance proposals and listen to community concerns early in the process can result in massive backlash and wasted time and funds when plans have to be suspended or even cancelled. Oakland was forced to scrap most of the planning for its Domain Awareness Center and scale the project back considerably after community members protested the misleading mission statement and lack of transparency for the project. Engaging with the community before deciding whether to go forward with surveillance proposal can help in avoiding a similar mistake.

5.1 Conclusion

The Ethical challenges and issues on the use of surveillance technology is increasing with the advent of new technologies, surveillance in itself is a serious and growing issue, it's essentially a problem of unequal power. The usual reform solutions, such as codes of professional ethics, laws and regulations, give only an illusion of protection. Nigeria is planning to ramp up surveillance on her citizens, the question is how does a nation that has no Data Privacy laws or legal provision for interception seek to monitor communication.

References

http://en.wikipedia.org/wiki/Surveillance

http://www.iep.utm.edu/surv-eth/

http://ww2.kqed.org/news/wp-content/uploads/sites/10/2014/11/report.pdf

http://www.publications.parliament.uk/pa/ld200809/ldselect/ldconst/18/