International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 8 Issue 4, Jul-Aug 2024 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Ubiquitous Technical Surveillance: An Introduction

Paul A. Adekunte[1], Matthew N. O. Sadiku[2], Janet O. Sadiku[3]

[1]International Institute of Professional Security, Lagos, Nigeria
[2]Roy G. Perry College of Engineering, Prairie View A&M University, Prairie View, TX, USA
[3]Juliana King University, Houston, TX, USA

ABSTRACT

Ubiquitous technical surveillance (UTS) is the collection and long-term storage of data in order to analyze and connect individuals with other people, activities, and organizations. Our data and as well as associated metadata are valuable commodity for commercial organizations who use it to discover what their clients/customers want, shape how they market the product, and serve it up in a way that will make you buy it. Metadata is the summary and the description about your data which is used to classify, organize, label, and understand data, making sorting and the searching for data much easier – this makes the huge amounts of data created and collected across an enterprise to be manageable by organizations. Unprotected metadata can be revealed to the wrong person such as hackers, malicious competitors, and cybercriminals. This paper delves into some of the challenges of ubiquitous surveillance and the way forward.

KEYWORDS: *Ubiquitous surveillance, data, metadata, covert, overt, ubiquitous computing, UTS threat vectors, telematics data*

How to cite this paper: Paul A. Adekunte | Matthew N. O. Sadiku | Janet O. Sadiku "Ubiquitous Technical Surveillance: An Introduction" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-8 | Issue-4, August 2024, pp.231-239, URL: www.ijtsrd.com/papers/ijtsrd67144.pdf

IJTSRD67144

INTRODUCTION

Surveillance is used by investigators as aid in achieving investigation objectives and the method varies with the requirements of the case. For surveillance operation to succeed, there is need adequate preparation in the areas of selection of personnel, administrative and logistics support. Personnel security, protective security, physical security, and interrogation among others cannot be successfully carried out without surveillance. In other words, surveillance is a key factor in investigation and is imperative that personnel to be used are well trained and grounded in the state of the art.

Ubiquitous surveillance is the unilateral collection of data on people with sensors embedded in their everyday environment. This can be enabled by progress in ubiquitous computing, surveillance is penetrating activities used to be regarded as private. With browsers, phones, credit cards, CCTV, e-mail, social media, telecommunications, television and entertainment media, digital documents, and health records already tapped – making it harder to find the sphere of life where data are not collected, indexed, distributed, searched, and inferred. The level of control is grossly inadequate and meaning that ubiquitous surveillance is among the most alarming developments of our present time [1]. Governments and corporations are known to collect, store, and analyze the massive amount of data we chuff out as we move through our digital lives – this is often without our knowledge and consent. Whether we admit it or not, it should be noted that we are under mass surveillance. The collection of metadata on people means putting them under surveillance [2].

WHAT IS SURVEILLANCE?

Surveillance can be defined as a close watch, or a close observation method of collecting information about a person, group of persons or place, the object of which is to prevent crimes. This plays a vital role in many activities of law enforcement agents.

OBJECTIVES OF SURVEILLANCE

The objectives of surveillance are:

- To stop an illegal activity.
- To refute confirm an allegation.

- To investigate the reliability of persons to be employed in a sensitive Government Department (i.e. vetting).
- To discover agents, hoodlums, informants, contacts and their secret meeting places.
- It is used during investigation to gather information about a suspect before a search warrant is executed.
- To track down a criminal.
- To obtain lead upon which to base further investigation.
- It is used to provide protection for a V.I.P.
- To identify associates of suspects.
- To identify patterns of activities.
- To study the detailed movements of target.
- To discover their hide-out.
- To study the character of suspects.
- To know the reliability of human sources.
- To obtain photographs of a suspect.
- To obtain the proper description of the suspect.
- For tactical reasons.

CONCEPT OF UBIQUITOUS TECHNICAL SURVEILLANCE (UTS)

The United States Government in 2017 developed the Ubiquitous Technical Surveillance (UTS) to describe the threat posed by governments worldwide using technology to track the movements of their citizens and reconstruct their activities over time. Our data is stored indefinitely, and of which the records are accessible. Ubiquitous technical surveillance data can be used to forensically reconstruct events, no matter how long ago they occurred. Ubiquitous technical surveillance is said to be organized into five pathways for collection, which is also referred to as the five UTS Threat Vectors. These are [3]:

1. Online: anything and everything that we do online create a fingerprint that is as unique as those on our fingers. Online UTS Threat Vector includes all the data available about us online as well as the info generated by the devices used to access the internet. Information can be found out about us through the use of simple internet searches, data we generate when we interact with websites, search engines, apps, software programs, and much more. From the internet browser, to Advertising IDs (Ad-IDs), the Online UTS Threat Vector is a goldmine for advertisers who want to know what you like and are searching for. This however, provides enough information to help identify you based on your online habits. This fingerprint allows an advertiser to be able to find out/pinpoint your location, activities, and patterns, to personalize their offers to you – giving advertisers insight into your use of the internet.
2. Electronic: first and foremost, we need to get connected for us to use the internet. Electronic UTS Threat Vector does not just cover the Wi-Fi signals generated by our smart devices and the Internet of Things, but also radio frequencies (how cell phones communicate with cell towers) and telematics data created by our vehicles (also known as fleet tracking or GPS vehicle tracking) [4]. Some of these threat vectors include Bluetooth connections, GPS information, RFID, and paired devices like smartwatches or fitness trackers. This as well gives adversaries a great deal of information about you personally, such as your phone's IMEI or a computer's MAC address, such that your devices can be picked out from vast sea of other devices in the data.
3. Visual-physical: the CCTV cameras that are installed at your neighbor's smart doorbell, the Visual-Physical UTS Threat Vector incorporates all the mechanisms that collect data about you and what you look like a you move about the world in real life. It also involves processing algorithms such as facial recognition and gait analysis. CCTV cameras are now being installed in major cities in the world in order to investigate crime, deter citizens from unrest, and to track the movements of people, as in Figures 1 and 2.
4. Financial: the Financial UTS Threat Vector covers data generated by financial transactions. After the 9/11 attack, banks worldwide collaborated on counter-terrorist financing efforts, which was to help banks and governments to track all the money moving worldwide. Swiping, tapping, inserting a card to pay, paying bills on a banking app, sending money through another app, and writing a check that eventually gets deposited into an account – all create a trail of data and attribution that can help to keep you safe from fraud.
5. Travel: the Travel UTS Threat Vector involves all the data created by travel activities such as flight itineraries, location searches in your GPS, connections and communication with travel companions etc. Travel UTS Threat Vector help adversaries identify where we go, how and when we go there, and with whom we meet when we get there.

Everything we do is being tracked and registered by technology, e.g. our location is constantly monitored by our phone company cum those we communicate with and when, where and what we spend our money

on are noted by our banks, our health can be tracked by sports watches, as in Figure 3. Technology to track/monitor and register everything is improving all the time and 5G telephony and the Internet of Things will only make things worse or rather better – as ubiquitous surveillance will make life more easy, safe, and improve our lives in the area of early warning of outbreaks of diseases and the spread of epidemics, etc [5].

UTS presents the most acute, generalized threats and opportunities facing the broader Intelligence Community (IC), Department of Defense (DoD), and the United States Government (USG). Foreign intelligence and security organizations capitalize on marketing infrastructure as well as other means to compromise the safety and security of US service members, IC officers, and others to collect and exploit US interests [6].

EXAMPLES OF SURVEILLANCE

A few examples of electronic surveillance are: wiretapping, bugging, videotaping, geolocation tracking, as shown in Figure 4, data mining, social media mapping, and the monitoring data and traffic on the internet. Generally speaking, surveillance could be electronic or fixed. Surveillance is the act of observing another in order to gather evidence. It is one of the common methods used by law enforcement official to investigate suspects and gather evidence – which could be with the knowledge of the person being surveilled (overt surveillance) or without (covert surveillance). Fixed surveillance includes covert surveillance of individuals in-person, also referred to as "stake-outs." Surveillance/security cameras are not all sunshine and rainbows, they come with challenges and considerations that businesses must navigate. Other forms of classification of surveillance are direct, preconstructive, and reconstructive – in which case, direct is covert, preconstructive is more public, and reconstructive is the reviewing of information and evidence gathered from the other two techniques [7, 8, 9]. Other methods of surveillance also include: satellites, and video cameras.

SURVEILLANCE EQUIPMENTS

Surveillance equipment refers to electronic surveillance device, hardware, or software that is capable of collecting, capturing, recording, retaining, processing, intercepting, analyzing, monitoring, or sharing audio, visual, digital, location, thermal, biometric, or similar information or communications specifically associated with, or capable of being associated with, any specific individual or group, as shown in Figure 5; or any system, device, or vehicle that is equipped with an electronic surveillance device, hardware, or software [10]. Overt operations could include political alliances, economic measures, and "white" propaganda, and while covert operations include, but not limited to, clandestine support of friendly foreign elements, "black" psychological warfare, and inciting revolution. Surveillance is the covert observation of people, places and vehicles, which law enforcement agencies and private detectives use to investigate allegations of illegal behavior, which involves major risks. Some of these are [11]:

- Electronic monitoring: this is also called wiretapping – which is the surveillance of email, fax, internet and telephone communications. In the US a court order is required to proceed based on a US government affidavit.
- Fixed surveillance: also known as "stakeout," requires officers to surreptitiously observe people and places from a distance. This could involve the one- and two-person surveillance methods, however, the two-person approach is considered more desirable by Michael Palmiotto an author and criminal justice professor.
- Stationary technical surveillance: in this case the investigator installs a hidden camera and recording equipment in a parked car. This is called unmanned surveillance.
- Three-person surveillance: this method is a bit complex, and of which officers can change positions more often, in order to reduce the possibility of detection. This is also referred to as the ABC method.
- Undercover operations: this is another form of surveillance in which the officer plays an active role in revealing criminal activities.

The designed formations for all cases are [12]:

1. One-man formation:

- This is where one man (one person) monitors the target and walks behind the target.
- This kind of surveillance is extremely difficult for one man and should be avoided if possible.
- The target must be kept in view at all times.
- When walking on the opposite side of the street, the officer should keep almost abreast of the target.
- It is necessary at all times to be close enough to immediately observe the target if he enters a building, turns to a corner or makes any funny moves.

2. Two man/bi-lateral/leap frog/AB formation:

- Two individuals perform the process of surveillance and walk behind the target alternatively.

- The use of two officers affords greater security against detection and reduces the riskof losing the target.
- The officers change positions vertically and horizontally according to the degree of density, target's movement, the wideness or narrowness of the street/roads.
- One officer leap-frog ahead of the target as appropriate while the second officer drops behind.

3. ABC/Triad or Quatro formation:

- The use of three officers further reduces the risk of losing the target and also affords greater security against detection. Even if one of them is detected, he can easily drop out without affecting the integrity of the operation.
- Individuals "A" and "B" (lead and back-up) walk behind the target while individual "C" (Rover) walks on the other side parallel to him so that he can observe his movements and directions and give the signal agreed upon to other individuals.
- All the officers involved in the operations should be properly focused and pay attention to the target's intentions.
- Individual "D" has to watch out in order to reveal any counter surveillance, moving behind the target.

4. Vehicular surveillance: In this case two or more vehicles are required for vehicular surveillance. The number of participants in each car must not be more than four and not less than two.

- Car "A" should remain some distance behind target's car, with one or two cars in-between.
- Car "B" remain one car behind "A" while car "C" could take the position of a rover if the lane permits such.
- Like the foot surveillance (ABC formation) cars "A", "B", "C" can alternate positions to avoid recognition and even drop one occupant out of their numbers when the need arises.
- All the cars involved should maintain discreet communication among themselves in order to achieve success.
- Where possible the target's car could be planted with tracking device for easy location.

Furthermore, surveillance equipments are tools used by the surveillance industry, police, military intelligence, and national security for individual surveillance and mass surveillance. This is as compiled by Steven Ashley [13]:

- Primary electronic: digital still and video cameras (CCTVs), GPSs for tracking, electronic toll takers, computer surveillance, phone tapping, cell phone monitoring, voice, facial features, walking gait and other biometric characteristics, covert listening devices or "bugs" – tiny hidden microphones and short-range radio transmitter, directional microphones.
- Primary chemical: artificial noses, chemical markers like UV markers, DNA sensors – Biochip etc. for screening tiniest traces of body material.

Others: airplanes – unmanned aerial vehicles and satellites, night-vision goggles or telescopes, laser beam bounced off a window to record vibrations in the pane from conversations in the room, discarded items containing information like phone bills, credit-card statements and computer hard drives (using digital forensics).

When electronic means is combined with internet features (ubiquitous computing, IoT) and enhanced by artificial intelligence (AI) analysis methods readily lend themselves to mass surveillance. AI can now process every frame and give real-time analysis to prevent lethal crimes, introducing unprecedented capabilities and efficiency, as shown in Figure 6 [14]

CHALLENGES TO UBIQUITOUS TECHNICAL SURVEILLANCE

We are presently in the era of pervasive surveillance, where organizations are faced with serious challenges in maintaining their privacy and security. Some of the challenges facing ubiquitous technical surveillance are that [15]:

- Prime targets for corporate espionage are the CEOs, politicians, corporate executives (i.e. public figures), and celebrities because of their influential positions, as a result of their potential access to sensitive information, and confidential business plans.
- Competing organizations or actors with malicious intent can make use of surveillance techniques to gain unfair advantage, intercept trade secrets, or cause harm to targeted organizations.
- The risk of information leaks and unauthorized access to proprietary data poses a great threat to corporations – which can jeopardize a company's competitiveness and integrity.
- Privacy worries: the more data we gather, the more the feeling that someone is watching, raising the questions about those seeing and using our data, and of which companies could misuse our data for intrusive ads and unfair pricing. It could as well create data silos making it more likely for people to track us or even steal our personal information.
- Security risks: ubiquitous data is like an open door for cyber-attacks, hence the need to make it very secure.

- Data accuracy: the keeping of data accurate is tricky when it comes from many places, as false information or mistakes can slip in, which could result to bad decisions or unreliable results.
- Data overload: this leads to strain on our computers and storage systems due to too much data to handle, making it hard to get useful insights quickly.
- Standardization issues: lack of standard rules in handling data makes it difficult to combine data from different sources for useful analysis.
- Ethical and legal dilemmas: when figuring out who owns the data and what could be done with it can be very confusing, since different places have different rules, such that navigating this legal maze can be challenging for organizations, leading to disputes and lawsuits.
- Environmental impact: data centers handling these data, use a lot of energy, which leads to environmental issues like climate change
- Social and behavioral changes: when we are aware that people are constantly watching us, the tendency is that we change how we behave.
- Algorithm bias: algorithms that analyze data learn from the past, and if the past is biased, then the programs can make biased decisions. This could worsen existing inequalities, like in the justice system or when getting loans.
- Tech challenges: this requires the input of many experts, i.e. from tech-savvy folks to ethics experts, legal professionals, and policymakers [16].

WAY FORWARD

The way forward is an integrated set of purpose-built technologies working together to identify and respond to advanced threats, since deploying multiple technologies that cannot share intelligence or coordinate a response doesn't address the problem. In addition, security professionals require more rigorous and intelligent inspection capabilities that extend in-line products, and bring them together as a cohesive solution set without impacting performance or accuracy [17, 18].

CONCLUSION

It is through Ubiquitous Technical Surveillance (UTS) that the adversaries get deep insight or information into how businesses and organizations operate. Datasets overlaid with any combination of the five UTS Threat Vectors can be used to construct a vivid picture that describes somebody's pattern of life or business operations. When this is done, then cyber attackers can use it to carry out anomalous activities in order to thwart missions or disrupt business plans. Surveillance technology when used correctly and ethically, can be a useful tool to improve and enhance security, improve employee productivity, and inform market research, among others. However, despite the numerous usefulness of surveillance technology, it has it's dark side or trade-offs such as the difficulty in preventing one's data from being collected, or one's face being saved in an unknown database. There is also the concern on privacy violation that could lead to privacy and compliance concern [19, 20].

REFERENCES

[1] Antti Oulasvirta et al., "*Long-term effects of ubiquitous surveillance in the home*," September 2012, https://www.researchgate.net/long-term-effects-of-ubiquitous-surveillance-in-the-home

[2] Bruce Schneier, "Ubiquitous surveillance and society," June 29, 2017, *IEEE Technology and Society,* https://technologyandsociety.org/ubiquitous-surveillance-and-society

[3] "What is UTS?" https://www.ridgelineintl.com/what-is-uts

[4] "What is telematics & how do telematics systems work?" (May 28, 2024), https://www.geotab.com/what-is-telematics

[5] Klaus Mogensen, Best case/worst case: Ubiquitous surveillance," February 24, 2022, https://cifs.dk/best-case-worst-case

[6] Gruber, C. W. et al., 2023, "Ubiquitous Technical Surveillance: A Ubiquitous Intelligence Community Issue," In: Gruber, C. W., Trachik, B. (eds), *Fostering Innovation in the Intelligence Community. Annals of Theoretical Psychology,* vol. 19, Springer, Cham, https://doi.org/10.1007/978-3-031-29807-3_1

[7] "Surveillance," October 2021, https://www.law.cornell.edu/surveillance

[8] "Business security with surveillance cameras: Pros and Cons," February 22, 2024, https://mammothsecurity.com/business-security-with-surveillance-cameras

[9] Jack Woerner, Janell Blanco, "Surveillance I Definition, Techniques & Methods," November 2023, https://study.com/surveillance-definition-techniques-and-methods

[10] "Surveillance equipment definition," https://lawinsider.com/dictionary/surveillance-equipment-definition

[11] Ralph Heibutzki, "Types of surveillance in criminal investigations," July 01, 2018, https://work.chron.com/types-of-surveillance-in-criminal-investigations

[12] "Surveillance," being a lecture presented to Nigeria Security and Civil Defense Corps on Investigative Course, at the Independent Corrupt Practices and Other Related Offences Commission (ICPC), Training Academy, Abuja, 20th May to 6th June, 2008.

[13] "Surveillance tools," https://en.m.wikipedia.org/surveillance-tools

[14] Sudeep Srivastava, (June 24, 2024), "How AI is transforming traditional surveillance systems," https://appinventiv.com/how-ai-is-transforming-tradiiional-surveillance-systems

[15] Walter G., "Ubiquitous Technical Surveillance concerns for corporate executives," 21 January, 2024.

[16] "Ubiquitous data: definition, challenges & how to manage," https://www.questionpro,com/

[17] David Finger, "Advances in advanced threat protection," April 25, 2016, https://www.fortinet.com/advances-in-advanced-threat-protection

[18] "Managing challenges and risks in ubiquitous IT systems," May 18, 2016, https://www.fortinet.com/managing-challenges-and-risks-in-ubiquitous-it-systems

[19] "Surveillance technology - Thoughtworks," https://www.thoughtworks.com/surveillance-technology

[20] Andy Greenberg, (June 12, 2024), "Medical-Targeted Ransomware is Breaking Records after Change Healthcare's $22m Payout," https://www.wired.com/medical-targeted-ransomware

Figure 1. Closed-circuit television.

Source:https://www.google.com/search?sca_esv=4fcc697e8d17e72f&sxsrf=ADLYWIL43DBE9sGUAT8M6Qig9FBgBmx_yA:1719227945925&q=images+on+ubiquitous+technical+surveillance+by+wikipedia&tbm=isch&source=lnms&fbs=AEQNm0Aa4sjWe7Rqy32pFwRj0UkW9NAzhPVmkAfB2zK1tnQfJ7YXLTPLGowL1aB4gvrdKmvT1VKZKA7Y-vAPWsSmEmd7CANB-Ivwj74YTa4EcvLAEU7kPaPmp2sH3bGLokZWpx8jf3bnThEzDTbSHZkAfWwnN3KW0k-bQY2JlD62aLpzwzj3-jXk7ajEAK8MMDRRy5e1Oj0C&sa=X&ved=2ahUKEwjowoSYj_SGAxXPT6QEHSoqAjcQ0pQJegQIDRAB&biw=1034&bih=539&dpr=1#imgrc=ZrJeEL1DOJu8eM

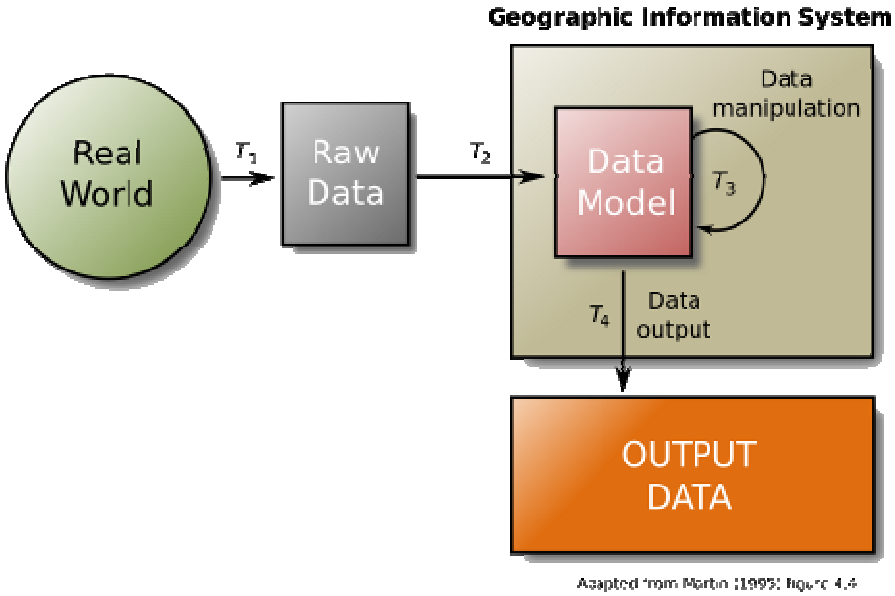

Figure 2. Geographic information system.

Source:https://www.google.com/search?sca_esv=4fcc697e8d17e72f&sxsrf=ADLYWIL43DBE9sGUAT8M6Qig9FBgBmx_yA:1719227945925&q=images+on+ubiquitous+technical+surveillance+by+wikipedia&tbm=isch&source=lnms&fbs=AEQNm0Aa4sjWe7Rqy32pFwRj0UkW9NAzhPVmkAfB2zK1tnQfJ7YXLTPLGowL1aB4gvrdKmvT1VKZKA7Y-vAPWsSmEmd7CANB-Ivwj74YTa4EcvLAEU7kPaPmp2sH3bGLokZWpx8jf3bnThEzDTbSHZkAfWwnN3KW0k-bQY2JlD62aLpzwzj3-jXk7ajEAK8MMDRRy5e1Oj0C&sa=X&ved=2ahUKEwjowoSYj_SGAxXPT6QEHSoqAjcQ0pQJegQIDRAB&biw=1034&bih=539&dpr=1#imgrc=BSpsc5AVAB34UM

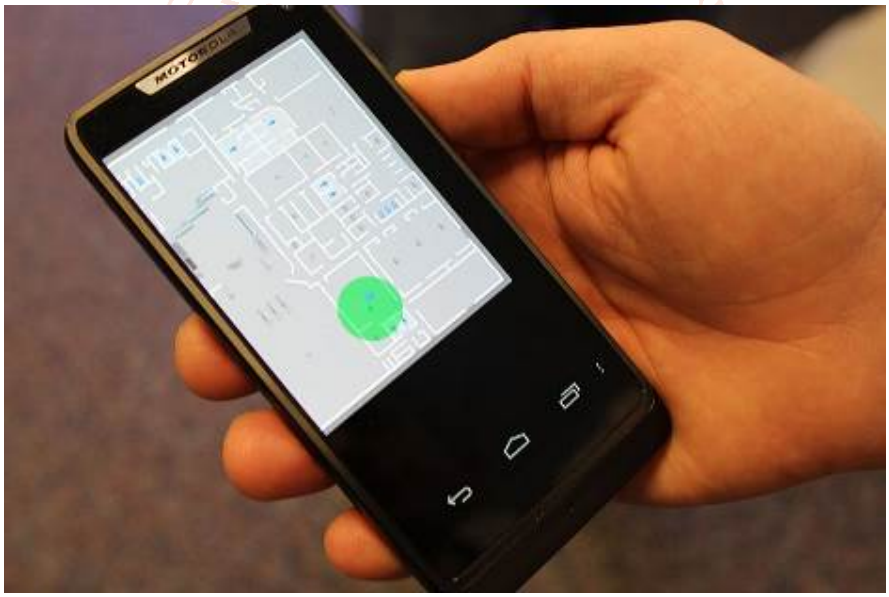

Figure 3. Mobile phone tracking.

Source:https://www.google.com/search?sca_esv=4fcc697e8d17e72f&sxsrf=ADLYWIL43DBE9sGUAT8M6Qig9FBgBmx_yA:1719227945925&q=images+on+ubiquitous+technical+surveillance+by+wikipedia&tbm=isch&source=lnms&fbs=AEQNm0Aa4sjWe7Rqy32pFwRj0UkW9NAzhPVmkAfB2zK1tnQfJ7YXLTPLGowL1aB4gvrdKmvT1VKZKA7Y-vAPWsSmEmd7CANB-Ivwj74YTa4EcvLAEU7kPaPmp2sH3bGLokZWpx8jf3bnThEzDTbSHZkAfWwnN3KW0k-bQY2JlD62aLpzwzj3-jXk7ajEAK8MMDRRy5e1Oj0C&sa=X&ved=2ahUKEwjowoSYj_SGAxXPT6QEHSoqAjcQ0pQJegQIDRAB&biw=1034&bih=539&dpr=1#imgrc=2YaIFcoZu-YhbM

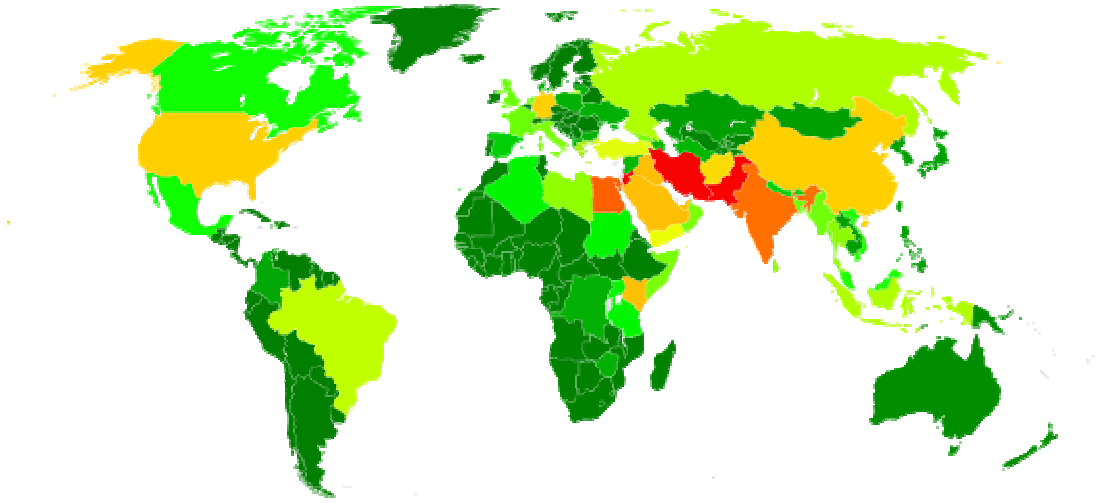

Figure 4. Mass surveillance in the United States of America.

Source:https://www.google.com/search?sca_esv=4fcc697e8d17e72f&sxsrf=ADLYWIL43DBE9sGUAT8M6Qig9FBgBmx_yA:1719227945925&q=images+on+ubiquitous+technical+surveillance+by+wikipedia&tbm=isch&source=lnms&fbs=AEQNm0Aa4sjWe7Rqy32pFwRj0UkW9NAzhPVmkAfB2zK1tnQfJ7YXLTPLGowL1aB4gvrdKmvT1VKZKA7Y-vAPWsSmEmd7CANB-Ivwj74YTa4EcvLAEU7kPaPmp2sH3bGLokZWpx8jf3bnThEzDTbSHZkAfWwnN3KW0k-bQY2JlD62aLpzwzj3-jXk7ajEAK8MMDRRy5e1Oj0C&sa=X&ved=2ahUKEwjowoSYj_SGAxXPT6QEHSoqAjcQ0pQJegQIDRAB&biw=1034&bih=539&dpr=1#imgrc=pM1sQMReKn4nrM

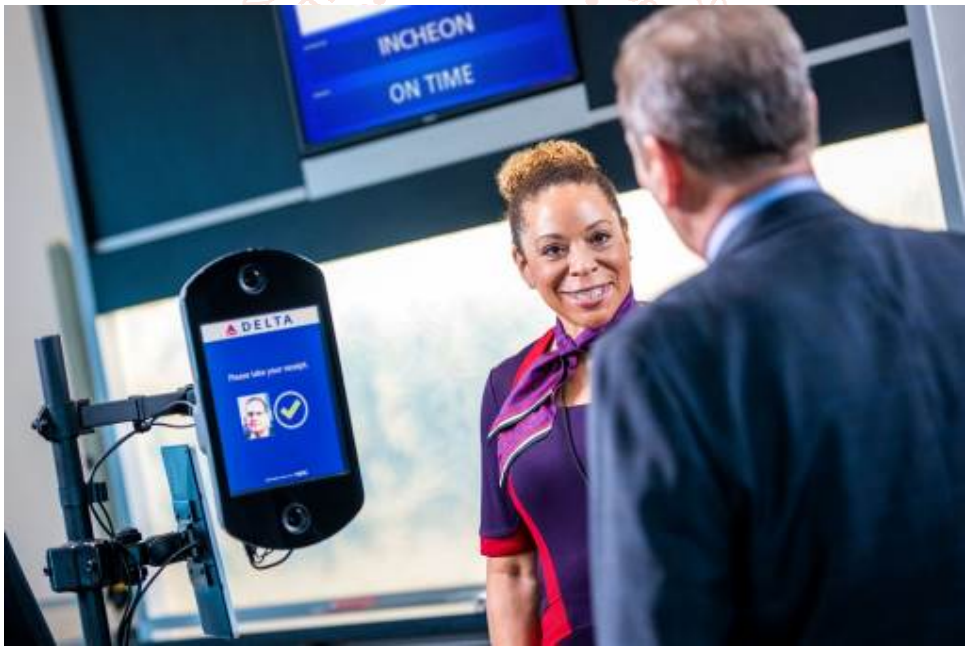

Figure 5. Facial recognition system.

Source:https://www.google.com/search?sca_esv=4fcc697e8d17e72f&sxsrf=ADLYWIL43DBE9sGUAT8M6Qig9FBgBmx_yA:1719227945925&q=images+on+ubiquitous+technical+surveillance+by+wikipedia&tbm=isch&source=lnms&fbs=AEQNm0Aa4sjWe7Rqy32pFwRj0UkW9NAzhPVmkAfB2zK1tnQfJ7YXLTPLGowL1aB4gvrdKmvT1VKZKA7Y-vAPWsSmEmd7CANB-Ivwj74YTa4EcvLAEU7kPaPmp2sH3bGLokZWpx8jf3bnThEzDTbSHZkAfWwnN3KW0k-bQY2JlD62aLpzwzj3-jXk7ajEAK8MMDRRy5e1Oj0C&sa=X&ved=2ahUKEwjowoSYj_SGAxXPT6QEHSoqAjcQ0pQJegQIDRAB&biw=1034&bih=539&dpr=1#imgrc=1RqHxjLTBktnRM

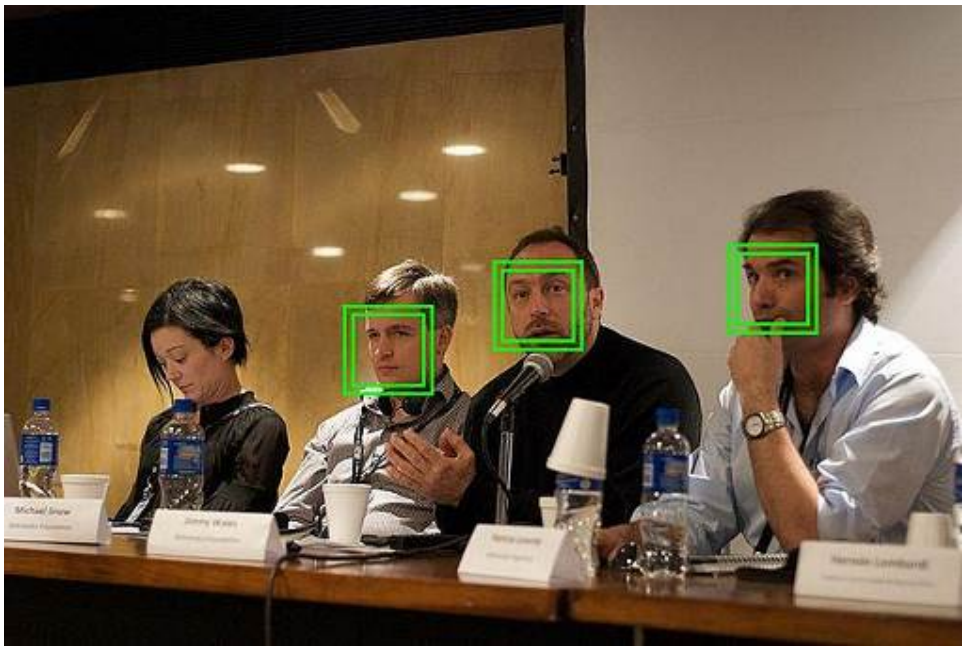

Figure 6. Artificial intelligence for video surveillance.

Source:https://www.google.com/search?sca_esv=4fcc697e8d17e72f&sxsrf=ADLYWIL43DBE9sGUAT8M6Qig9FBgBmx_yA:1719227945925&q=images+on+ubiquitous+technical+surveillance+by+wikipedia&tbm=isch&source=lnms&fbs=AEQNm0Aa4sjWe7Rqy32pFwRj0UkW9NAzhPVmkAfB2zK1tnQfJ7YXLTPLGowL1aB4gvrdKmvT1VKZKA7Y-vAPWsSmEmd7CANB-Ivwj74YTa4EcvLAEU7kPaPmp2sH3bGLokZWpx8jf3bnThEzDTbSHZkAfWwnN3KW0k-bQY2JlD62aLpzwzj3-jXk7ajEAK8MMDRRy5e1Oj0C&sa=X&ved=2ahUKEwjowoSYj_SGAxXPT6QEHSoqAjcQ0pQJegQIDRAB&biw=1034&bih=539&dpr=1#imgrc=e6N8vWmyfFoT9M