Received: 9 August 2020 | Revised: 29 October 2020 | Accepted: 13 November 2020 | Published on: 3 February 2021

DOI: 10.1002/spy2.142

SURVEY PAPER

WILEY

Mass surveillance: A study of past practices and technologies to predict future directions

Ben Underwood | **Hossein Saiedian**

Electrical Engineering & Computer Science, The University of Kansas, Lawrence, Kansas, USA

Correspondence
Hossein Saiedian, Information & Telecommunication Technology Center (ITTC), The University of Kansas, Lawrence, KS, USA.

Abstract

This paper aims to dispassionately examine the techniques and technologies of mass surveillance. We will study different approaches and technologies, including what each one surveils and how. We will also observe patterns and changes over time, and in doing so, we will seek to model the attributes exhibited by various methods. Finally, we will predict what next generation surveillance methods will look like, based on the attributes we have observed in past and current methods. Our key insights include: (a) mass surveillance methods share a number of common attributes, (2) we can analyze the expression of these attributes to predict future methods of mass surveillance, and (3) a likely next generation method will entail the monitoring of a communication platform with third-party assistance to collect large amounts of private communication data for future analysis.

KEYWORDS

governmental surveillance, industrial surveillance, mass surveillance, mobile devices, National Security Agency, privacy, social implications, surveillance technologies

1 | INTRODUCTION

Mass surveillance has been with us for thousands of years, though rapid technological advancements in the last hundred years have greatly increased the variety of methods used. By studying these methods and modeling the attributes they express, we can make an informed prediction of what next generation mass surveillance will look like.

Mass surveillance has long been a part of popular culture; however, it has often been presented in the context of science fiction. For example, in the 1927 silent film Metropolis, the workers of a future industrial city are closely monitored by their employer. In the 1998 film Enemy of the State, a manhunt is carried out with Global positioning system (GPS) tracking, satellite imagery, and closed circuit television (CCTV) cameras. These plot devices were chosen to lend fantastical elements of noir to their stories, but today they are less far-fetched.

Consider this sampling of news headlines from March 2017:

- President Donald Trump announced that he was wiretapped while President-Elect in late 2016. The Chairman of the Intelligence Committee of the House of Representatives explained that it was likely part of routine work by American intelligence agencies.[1]
- Mainstream news outlets discussed the whistleblowing website Wikileaks' publication of Central Intelligence Agency (CIA) hacking tools, including the ability to "make Internet-connected Samsung television sets secretly function as microphones."[2]

- Searches of mobile phones by US border agents, including demanding passcodes under penalty of detention, grew by approximately 500% in 2016. A first amendment attorney familiar with the increase observed: "They are building capacity to routinely search as many devices as possible."[3]
- The US Congress passed legislation to nullify Federal Communications Commission rules which prohibited Internet Service Providers (ISPs) from selling private data without permission. ISPs are now expected to sell web browsing histories to advertisers.[4]

But surveillance was not always a part of the national conversation. Much of the current interest in the subject can be traced to the 2013 publication of information from former National Security Agency (NSA) contractor Edward Snowden. Snowden's story captured the public's imagination because he provided thousands of pages of documentation to support his claims. As a result, the operations themselves may still take place in the shadows, but the public now knows of their existence.

Mass surveillance is observation that has been scaled up past some threshold in terms of the number of objects being surveilled, or the size of the surveilled area. It targets all individuals or objects that match a desired set of characteristics. Perhaps the first mass surveillance was the census by the Babylonians in 3800 BC. Another early method was enhancing one's view with a high ground position. Chinese military strategist Sun-Tzu advised in the fifth century BC that "you should occupy the raised and sunny spots."

Global mass surveillance began with a communications surveillance sharing agreement in the mid-1940s called UKUSA. Originally between Britain and the United States, UKUSA has since expanded to include Canada, Australia, New Zealand, and many others. The sharing allows each country to focus its surveillance efforts on a specific geographic region of the world.

In the United States, the primary communications surveillance agency is the NSA. The NSA has an annual budget of approximately $10 billion, and an estimated 40 000 employees.[5] Mass surveillance is also big business in the private sector. The Israeli company Cellebrite, the Italian company Hacking Team, and the German company Finfisher are major corporate players in the burgeoning industry of selling proprietary mass surveillance technologies to foreign governments.

The aims of mass surveillance are many. What was once primarily a military and governing tool is now in use by marketers, scientists, local law enforcement, insurance companies, and human resources departments. Where endeavors rely upon information about a given population, whether inhabiting a particular geographic area or matching some other attribute, mass surveillance methods and providers exist to collect and analyze that data.

Legal issues are important to consider, but outside the scope of this article. A comprehensive collection compiled by David Gray and Stephen Henderson[6] explores the topic extensively. Such writings by leading researchers on surveillance law can be a thought-provoking asset for government officials, policy makers, academics, and law students.

2 | SELECT MASS SURVEILLANCE METHODS AND TECHNOLOGIES

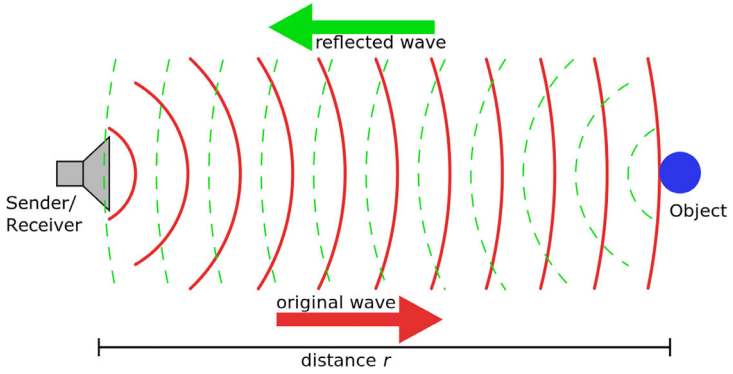
2.1 | Informant networks

A classic example of a non-technical form of surveillance is the recruitment of an informant. Informants have existed if any types of competing groups have existed. Formalized informant systems were created and used by the ancient Greeks, the ancient Romans, the English in the Middle Ages, and the 19th century French.[7] The Romans actively recruited grain merchants to report on domestic matters, since supply routes carried them across the Mediterranean to the far corners of the empire.[8]

This practice has continued throughout history, with a dramatic example occurring in 1980s East Germany. By 1989, the Stasi secret police of East Germany had built up a network of hundreds of thousands of civilian informants to monitor for domestic political dissent. The German government today believes there could have been as many as 500 000 informants in the network, and a former Stasi colonel estimates the number could be as high as 2 million if occasional informants were included. East Germany had a total population of 16 million, meaning that at one time, up to 12.5% of its population was formally recruited and organized for confidential informing purposes.

The US Department of Homeland Security's (DHS) "If You See Something, Say Something" campaign is a present-day example of an attempt at recruiting such a network, even if more loosely organized. The DHS officially implores "everyday citizens" to participate in its domestic security mission by "recognizing and reporting suspicious activity": "If you see

FIGURE 1 An active sonar system[11]



something you know shouldn't be there—or someone's behavior that doesn't seem quite right—say something." The DHS's recruitment message includes marketing taglines such as "Homeland security begins with hometown security".[9]

2.2 | Postal mail tracking

In the early 1800s, the United States Postal Service (USPS) began what would become a surveillance program called Mail Covers. When requested by a law enforcement agency, the USPS will record and share the outside of a target's letters and packages.

From 1952 to 1973, the CIA conducted a mass mail-opening program called HTLINGUAL. Originally for foreign intelligence, Richard Nixon expanded the mail-opening surveillance to include members of the domestic anti-war movement.

In 2001, the USPS began the Mail Isolation Control and Tracking program, an automated imaging system which photographs the exterior and stores the path of every piece the USPS handles.

2.3 | Sonar

Sound is a pressure wave that propagates through a medium. Human ears are best adapted to detecting sound in air; however, air is not the only medium through which sound propagates. In 1490, Italian artist and inventor Leonardo da Vinci wrote "If you cause your ship to stop and place the head of a long tube in the water and place the outer extremity to your ear, you will hear ships at a great distance from you."[10] This is the first recorded use of what would eventually become known as sonar.

Sonar is a technology for the monitoring of sound underwater and is in fact an acronym standing for SOund Navigation And Ranging. In 1906, American naval architect Lewis Nixon invented a sonar device for detecting icebergs. In 1915, French physicist Paul Langevin invented the first sonar device for detecting submarines.

Up until this time, all implementations of sonar had been passive, meaning that they were listening devices only. By 1918, both Britain and the United States had developed active sonar systems. Active sonar generates sound and listens for its reflection, which allows it to more accurately measure an object's position. Using the knowledge that sound travels through water at approximately 1500 m/s (approximately 4.5 times faster than through air), active sonar measures the time between sound generation and reflection and calculates from that time the distance of the reflector.

In the past hundred years, sonar technology has continued to be used and refined. Today, the fishing industry uses it to surveil for schools of fish. Oil and gas explorers use it to map the ocean floor. Militaries use networked arrays of sensors to surveil large areas of ocean for foreign vessels. There is even a handheld version for use by divers in low visibility conditions. A basic sonar system is shown in Figure 1.

2.4 | Radar

In the 1860s, James Clerk Maxwell theorized that electricity, magnetism, light, and radio waves are all different manifestations of electromagnetic radiation. Twenty years later, Heinrich Hertz demonstrated that radio waves do indeed exist, and that they can be reflected by metallic objects just as light can.

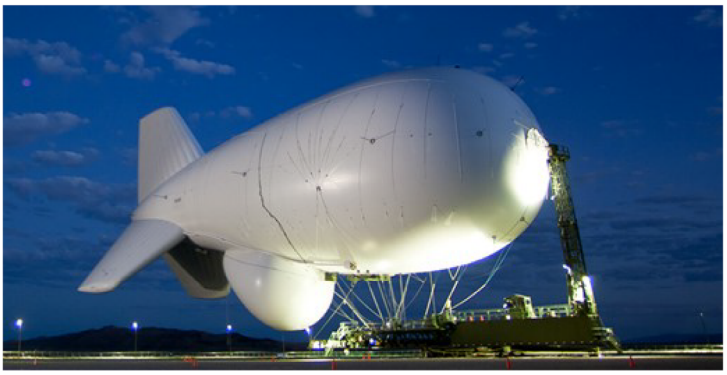


FIGURE 2 JLENS aerostat[13]

The United States, Germany, the United Kingdom, France, the Netherlands, Italy, the USSR, and Japan all developed radar independently in response to the emergence of long-range bombing aircraft in the 1930s. Systems were mounted on land, air, and sea platforms, and were primarily used to surveil for aircraft and surface naval vessels.

One interesting modern implementation is aerostat-mounted radar, such the Army's JLENS system or the US Customs and Border Protection's TARS system. Aerostats are moored high-altitude balloons that enable operators to aim the radar outward as well as downward, while avoiding the frequent refueling required by aircraft. US Customs and Border Protection uses the TARS system along the southwest border of the United States as part of a drug smuggling interdiction effort.[12] Figure 2 shows the JLENS system.

Characterized as a blind technology because it can detect objects but not visually identify them, radar has found civilian use in systems such as weather analysis, road traffic monitoring, and collision detection.

2.5 | Telegraph intercepting

The first form of electrical communication was the electric telegraph. The first working prototype was in 1774, and by the 1830s, enough incremental improvements had been made for telegraph systems to start seeing commercial use, especially along railways. The value of the near-instantaneous communication technology was undeniable, and it soon saw fast adoption across the world. The age of telecommunications had begun.

In 1850, an undersea telegraphic cable was laid between France and England. By 1861, telegraph lines connected the west and east coasts of the United States, and soon after, telegraph machines started appearing in post offices. By 1902, the entire world was encircled by undersea telegraphic cables.

By 1940, over 191 million telegraph messages were sent and received in the United States. That same year, the US Army began surveillance of the communication platform. In response to the breakout of war in Europe in 1939, all international telegrams passing through Washington, DC, New York, NY, and San Francisco, CA were surveilled. This was accomplished not through technical means, but by merely compelling the three major American telegraph companies, Western Union, AT&T, and Postal, to provide them.[14]

The war ended in 1945, but rather than ending telegraphic surveillance, the program was expanded. Under Project Shamrock, all daily telegraphic data to, from, or transiting the United States was surveilled. It was again accomplished with the cooperation of the major telegraph companies, and at the height of the operation, 150 000 messages per month were analyzed by intelligence personnel. The program continued until the mid-1970s, when it shut down under pressure from a Senate investigation. By this time, however, use of the telephone had far eclipsed that of the telegraph.

Technical wiretapping also evolved to covertly monitor telegrams by physically tapping the telegraph wire anywhere along its length, like how one might tap a maple tree to collect syrup. For mass surveillance purposes, however, compelling the cooperation of major telegraph companies was a far more scalable solution.

2.6 | Landline telephone tapping

In 1667 Englishman Robert Hooke created a rudimentary version of a telephone in which sound was projected as mechanical vibrations through a taut wire. In the mid-1800s, various European inventors demonstrated the transfer of sound through electromagnetism, referring to it as a speaking telegraph or sound telegraph.

In the 1870s, improvements were being made at a rapid pace by Elisha Gray, Alexander Bell, Thomas Edison, and others, with the master patent being issued to Bell in 1876. A critical enhancement came with the invention of the telephone switch by Hungarian Tivadar Puskas. The switch allowed for the scaling up of telephone technology through the formation of exchanges, and eventually networks.

The first commercial telephone services were set up in 1878 and 1879 in New Haven, Connecticut and London, England. By the mid-1880s, the United States had a network of inter-city telephone lines and exchanges in every major city. After World War II, user adoption and network build-out continued to expand. This network was known as the Public Switched Telephone Network (PSTN), also referred to today as Plain Old Telephone Service.

Surveillance of calls on PSTN was generally done via an adaptation of the original telegraph wiretapping method. A mechanical connection or bridge was made by a technician between the monitoring and monitored telephone lines, usually inside a local switching station where the two lines were in enough proximity to each other.

The age of digital telecommunications began with the invention of the transistor by Bell Laboratories in 1947. This and other digital enhancements such as switching circuits in the 1950s and electronic switching in the 1960s led to increased capacity and higher quality service. It also necessitated an evolution of call surveillance technologies.

This would prove to be a boon to intelligence and law enforcement agencies however, since tapping on the digital platform was far simpler and could be ordered remotely once the base capability had been established at a switching station. The first digital telephone wiretapping technology was created by the BellSouth Corporation in 1995. Its patent application described it as a "network-based solution to communications monitoring so as to provide monitoring of communications regardless of the physical locations of the monitoring and monitored lines." It did not require additional on-premises equipment, and its intended users were employers (to monitor customer service workers and salespeople) and law enforcement personnel.[15]

Another method called pen register tapping collects various activity information, such as calls to and from a number, but specifically excludes the contents of calls. This same non-call-content data can also be collected by simply requesting or requiring it from a telephone company's billing department.

2.7 | CCTV

In 1608, Hans Lippershey used his experience as a maker of eyeglasses to create the first telescope. Over the next several years, it would be used by Galileo Galilei and Johannes Kepler to make great leaps in the field of astronomy, with up to 30 times magnification.

The design was improved for hundreds of years, including the invention of the first practical binoculars by J.P. Lemiere in 1825. Essentially side-by-side telescopes, binoculars provided a wider field of view and a sense of depth, for both terrestrial and astronomical viewing. The ability to see farther than one could with the naked eye enhanced surveillance of distant surroundings, such as watching for approaching armies or counting approaching ships, especially when combined with a high-ground viewing position.

The invention of the photograph by Nicephore Niepce in France in 1816 meant that optically observed objects could for the first time be recorded by technical means, albeit in still form. The process was improved throughout the 1800s by Louis Daguerre (daguerreotype), Henry Fox Talbot (calotype), Desire van Monckhoven and Richard Leach Maddox (dry plates), and George Eastman (paper film and celluloid).

Photography meant the watcher was no longer required to remember or draw what they saw, and as such, it aided in the accurate communication of what exactly was seen. A picture, as they say, is worth a thousand words.

The advent of motion photography in the late 1800s enhanced surveillance further. It built upon the benefits of still photography by adding motion to the list of characteristics that no longer had to be remembered or described. In addition, a motion recording of surveillance objects has a greater chance of capturing temporary changes than still photographs taken over the same time period.

By 1893, Scotsman William Dickson and American Thomas Edison had developed what they called a kinetograph camera and the accompanying kinetoscope projector to play back the film recorded by the kinetograph. They used a frame speed of 30 frames per second. As Edison explained, "I have been able to take with a single camera and a tape-film as many as forty-six photographs per second … but I do not wish to limit the scope of my invention to this high rate of speed … since with some subjects a speed as low as thirty pictures per second or even lower is sufficient".[16]

In 1895, a phonograph was added for sound and the combined device was dubbed a kinetophone. In 1939, 8 mm handheld cameras made covert recording possible.

In 1942, German engineering company Siemens AG created CCTV to observe the launch of V-2 rockets (and they still develop CCTV systems today). "Closed circuit" refers to the system's transmittal of camera signals to a specific remote viewing platform, rather than broadcasting them. This allows for real-time remote observation, secured to selected observers. It also makes it possible for a single observer to surveil numerous locations. Whereas the telescope magnified human sight by allowing it to see farther, CCTV amplified it further by allowing it to be many places at once.

Many applications have been found for CCTV technology over the years. New York City installed CCTV cameras in Times Square in 1973 in an effort to deter crime, however the effect measured at the time was limited. Regardless, the use of CCTV by governments for crime prevention spread, in part due to its low cost in comparison to expanding police departments.[17] Homes and businesses also widely implement the technology, and more recent studies show greater efficacy for crime prevention.[18]

Criminals have also found uses for CCTV. One example is the illicit and covert installation of cameras at ATMs for use in tandem with a card skimming device. The skimming device reads a card's number and other information from the card's magnetic stripe, but the PIN is obtained by aiming a camera at the keypad to watch the cardholder enter it.

CCTV also allows industrial manufacturing processes to be monitored from a safe distance. Installations on roadways are used to detect congestion and accidents, and even enforce traffic laws such as with the use of automated red-light cameras.

By 2011, the number of CCTV cameras in the United States had grown to an estimated 30 million.[19] In the same year in the United Kingdom, the number of CCTV cameras was estimated at one for every 32 people, with the average UK citizen being seen by 70 CCTV cameras per day.[20]

Present-day advances in image resolution, camera miniaturization, and wireless signal transmission are continuing to fuel the adoption of CCTV systems worldwide.

2.8 | Audio processing software

The coupling of modern computing with the processing of audio signals has led to several interesting and powerful surveillance technologies.

In the early 1990s, in response to the highest per capita murder rate in the United States, seismographic software techniques were applied to a network of five microphones in Menlo Park, California, to be able to locate the source of gunshots to within tens of meters. Modern gunshot detection systems with distributed sensor arrays are known as wide area acoustic surveillance. They are deployed in cities, airports, college campuses, and the like to listen for acoustic signatures produced by muzzle blast or shock waves that occur as projectiles travel through the air. Some systems can identify the type of round fired in addition to its location.

Speech recognition software began with the ability to recognize around 10 words at Bell Labs in the 1950s. By the mid-1980s, IBM had developed a voice activated typewriter with a vocabulary of 20 000 words. Today, the technology is ubiquitous. Google Voice Search supports 30+ languages, Apple's Siri digital assistant is deployed on hundreds of millions of iPhones, and Amazon's voice-controlled smart speaker Echo is in more than 8 million homes.

Since at least 2006, the NSA has made successful use of speech recognition software to transcribe and index its new and archived recordings. Using this technology, 1 million recordings were indexed per day in 2006, allowing a single NSA linguist to perform keyword searches and select only relevant recordings to listen to, where relevancy is determined by a search keyword being spoken in the recording. Without this capability, only a tiny number of captured recordings could be analyzed.[21]

2.9 | Image processing software

Modern processing power allows pattern matching software to analyze high resolution digital image data in near real time. Snapchat's 160 million daily users are familiar with facial recognition technology, though they would refer to it by Snapchat's moniker "Lenses." Lenses is able to recognize key facial geometry points such as the location of the eyes, nose, and lips, and modify them for entertainment purposes, such as to enlarge eyeballs, or add rabbit ears. Most impressively, the modifications move in time with the input video, at 24 frames per second.

This same technology is the evolution of facial recognition software development that began in 1964. In 1997, the first commercial systems were put in use at banks and airports to aid security. By 2006, the recognition algorithms were

nearly 100 times more accurate, with some able to outperform humans in recognizing unique faces.[22] Today, the security implementations have expanded to sporting events and other large public gatherings, and Facebook is beginning to use it for emotion detection.[23]

While facial recognition software may process video, the patterns it looks for reside in the two-dimensional images that make up the video. Gait recognition software, on the other hand, processes a three-dimensional signal, with the third dimension being time. It is the movement, or change between frames, that is analyzed for pattern recognition.

Gait recognition software development has been under way since the 1980s, with the aim of "fingerprinting" an individual by the unique way in which they walk. It is a sought after biometric due to being achievable at a distance and with lower quality CCTV footage and is only recently becoming reliable enough for use on a wider scale.[24] In 2016, research was published showing that unique gaits can be recognized from the reflection of WIFI signals, showing that video is not the only medium that can be analyzed to reveal the biometric.[25]

Automatic license plate reader (ALPR) systems, also known as automated number plate recognition, are another image processing technique used for surveillance. Purpose-built cameras are mounted to police cars, traffic lights, road signs, and bridges with the ability to record almost 2000 license plate images per minute. Optical character recognition technology then reads the plate from the image, cross references it with databases such as for stolen vehicles and bench warrants, and alerts law enforcement if a plate is suspect. Finally, whether a match is found or not, each image is stored in a database along with its time and location, and can be cross referenced with vehicle owner data, creating a searchable record of the movement of people over time.

Private companies also employ their own ALPR systems, to sell the data to auto lenders, insurance companies, and auto recovery professionals (the "repo man"), in addition to law enforcement. One private ALPR operator, Vigilant Solutions, had amassed a database of 2.2 billion images by 2015.[26]

2.10 | Making use of public data and shared data

Data are often collected from publicly available sources and repurposed. For example, a lender may collect new incorporation and business license data from public records and use it as a lead list for marketing new business loans. A building supply company may collect publicly available building permit information to market to the builders. More likely, however, a third-party data aggregation/lead generation company will create the publicly sourced lead lists for sale to the lender and building supplier.

It is also common for a business to sell data that its customers have shared with it. For example, the business lender may sell the contact information of its borrowers to companies that sell office furniture or computer equipment. A computer security conference organizer may sell attendee contact information to security solution providers.

These have all thus far been examples of the use of data for commercial marketing purposes, but marketing is also an important part of political campaigning. In 2014, 44 American political campaigns used the services of a company called Cambridge Analytica (CA), and in 2016 CA worked for the campaigns of presidential candidate Ted Cruz and eventual winner Donald Trump.[27] Former senior presidential adviser Steve Bannon was a member of the CA Board of Directors prior to his role in the Trump administration.

CA is a political data mining company that claims expertise in "behavioral microtargeting." They identify specific "psychographic" traits within target audiences, down to the level of specific individuals, and consult politicians on how to tailor their messaging differently for each one.[28]

Much of the behavioral analysis has been done by mining social media data. This technique was honed by CA parent company SCL, who in 2014 paid tens of thousands of participants roughly $1 each to complete an online personality profile, which included giving SCL access to the participant's Facebook profile. SCL scraped the demographic data, "likes," and friend lists from each Facebook profile, and using a technique called seeding, they also scraped the demographic data and likes of each of the participant's friends. This increased their data set from tens of thousands of individuals to unknown millions.[29]

CA also analyzes smartphone data that is shared with it, such as data from Ted Cruz's "Cruz Crew" mobile app. Of all official 2016 presidential candidate apps, Cruz Crew went the furthest to collect personal information. It tracked physical movements, copied the phone's contacts, and asked users to register with their Facebook login, which granted access to various demographic data including friends and relatives.[30]

FIGURE 3 The radar domes of the RAF Menwith Hill facility in England[32]

2.11 | Airwave surveillance

Airwave-based information systems consist of a transmitter and a receiver. Therefore, to eavesdrop on such a system, one can position their own receiver. A cooperative program between the United Kingdom and United States eavesdrops on global airwaves by placing receivers in a network of satellites.

The satellite-based receivers collect over-the-air signals such as radio and television (both broadcast and narrowcast), since such signals travel in a straight line until interrupted. Much of a signal cast horizontally from the surface of the earth will reach space, because any part of the signal that does not hit something will keep traveling away in a straight line rather than following the curvature of the earth. So in far less than 1 second, an over-the-air signal can be intercepted by a surveillance satellite in low earth orbit and transmitted back to a ground station such as the England's Royal Air Force Menwith Hill facility for analysis,[31] shown in Figure 3.

2.12 | Alternative cameras

Traditional cameras capture light, which is the part of the electromagnetic spectrum visible to the human eye. Other cameras work by measuring energies not in the visible spectrum and converting them to analogous visible signals.

Night vision devices can amplify visible light up to 50 000 times. They also measure the near infrared thermal energy emitted by objects.

Thermographic cameras see into the mid and far infrared ranges to detect emitted heat. These cameras have military and civil implementations, including medical diagnostics, firefighting, and building inspection systems.

2.13 | User action logging

In the context of modern computing, user actions are usually logged at some level of detail, and logs are kept for some defined period of time. Such logs can aid in troubleshooting, by allowing an investigator to piece together what events led up to a bug or other unintended outcome.

Logs can also aid in security. By allowing the attribution of events to a specific individual, they fulfill an investigative role and serve as a deterrent to bad behavior. In general, logs are required by any official security standard, and alerting systems such as Intrusion Detection Systems are often based off logs.

Logs of user actions can also benefit business decisions. System designers analyze who is using their system or website, how, and for how long, for the purpose of improving user experience or advancing other business interests. For example, if an e-commerce company wanted users to click through a sequence of web pages to order a product, they would study what percent of users leave or "bounce" from the website at each page in the sequence. They would then select a target page and attempt to reduce its bounce rate by changing some element of the page to encourage users to advance. They would then test the effectiveness of the change by serving up the new page for a randomly chosen 50% of page visitors

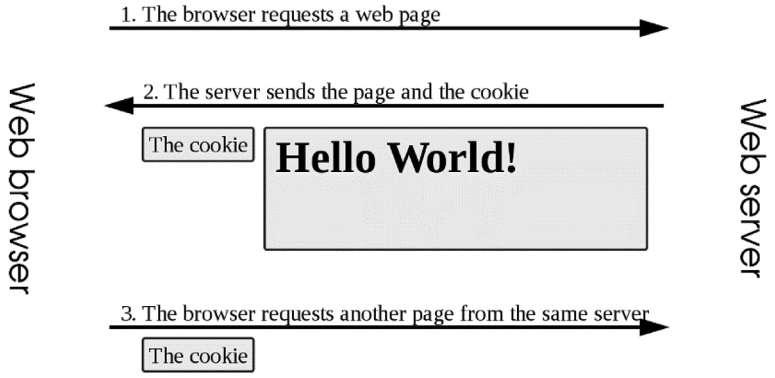


FIGURE 4 Cookie exchange interaction between a server and a browser[33]

(the test group), serving up the old page for the other 50% (the control group), and comparing the bounce rates of the two pages. The best version of the page (the one with the lowest bounce rate) is kept. And test group or control group membership is retained for the duration of the test, so individual users never have an incongruous experience by seeing both versions of the page.

Once a user has created an account at a website and logged into it, tracking user actions is simple. But not all users are willing to create accounts, and even a website that requires logging in may want to track activity on pages that do not require authentication, such as the home or contact page. To do this, developers use cookies.

A cookie is a small data file placed on a client machine by a website. The file is specific to a particular client/website pair, it can be accessed by the client or the website, and it contains data about the user and the user's activity on the website. For example, the cookie could contain a user's session ID, a list of the pages they have visited, information they have entered, and the cookie's expiration date. This allows a website to track its users without requiring them to log in, even tracking the same user across two different visits separated by a period of time, as long as they use the same device and browser for each visit. The website can use this to customize a user's experience by pre-populating information previously entered, or for analytics purposes as described in the bounce rate optimization example.

Cookies were developed in the mid-1990s and can be deleted or blocked in browser settings, but their use has become so ubiquitous that many modern websites will not function correctly without them. Thus, browsers are set to allow cookies by default.

Today, there are a variety of cookie types including session cookies (short term by nature), persistent cookies (longer term by nature), zombie cookies (recreated once deleted), secure cookies (transmitted over an encrypted connection), third-party cookies (belonging to a domain different than the website the user is on), and super cookies (associated with a top-level domain). Figure 4 shows an interaction between a server and a web browser, where the server transmits a cookie to the browser and the browser sends it back when requesting additional data. The *Wall Street Journal* reported in 2012 that America's top 50 websites placed some 64 pieces of tracking technology onto visitors' computers, totaling 3180 tracking files.

The European Union ePrivacy Directive requires websites in member countries to obtain consent from users for the use of many cookies.[34] In the United States, no analogous federal regulation exists.

2.14 | Cookie pooling

When banner advertisements first appeared on the web in 1993, they worked like print media advertisements in that they would display the same for all visitors to a web page with the exception of possible differences by time or geographic region. Advertisers were purchasing the exposure to all of a given web page's users.

In 1996, a company called DoubleClick began offering a proprietary analytical tool for advertisers called Dynamic Advertising Reporting and Targeting (DART), as well as brokering ad placement across numerous websites. These services helped banner advertisers to better target their ads, track their performance, and optimize it. DART employed a cookie that records what advertisement a user is shown, what URL it was shown on, and when. It also records the user's Internet Protocol (IP) address, allowing the advertiser to approximate the user's geographic location.[35] Eventually DoubleClick was acquired by Google, and versions of DART cookies are still in use today.

In 2003, Google introduced AdSense, an online display advertising network that is essentially an evolution of what DoubleClick started in 1996. A website that wishes to host advertising signs up to AdSense as a publisher and dedicates specific sections of their web pages to host banner ads. Google sends a bot to crawl the publisher pages to analyze them and determine what the content on the pages is about. If a publisher page contains the words "mileage," "transmission," and "4-cylinder," for example, Google's software may categorize it as being about cars. Advertisers separately upload their banner ads to AdSense. For example, Ford Motor Company may upload ads about its cars. Google then serves up the advertisements directly into the available spaces on publisher pages, and if a user clicks the ad, Google charges the advertiser a fee and pays a percentage of that fee to the publisher.[36]

AdSense has grown to become the dominant online display advertising network because of how effectively Google is able to target the placement of the advertising. In addition to context-relevant placement, such as placing a Ford ad on a page with an article about cars, Google can make placements relative to the specific user, such as their search history, general web-browsing history, location, or demographics. They can do this because they can pool together all of a user's DART cookies to construct a browsing history, and they will additionally have data on the user from their use of other services such as Gmail or the Google search engine. So for example, if a user spends a lot of time on the AdSense publisher car enthusiast website, but then visits an AdSense publisher food website, they may still be served ads about cars because the AdSense system has built a profile of the user's interests and activities. The ad may even be for a local Ford dealership, since the system is aware of the user's location through their IP address.

Perhaps the most interesting Google advertising targeting technique is called Remarketing. In 2010, Google began offering the Remarketing service, in which an advertiser lets Google track its visitors, for the purpose of advertising to a subset of those visitors across the web after they have left the advertiser's website.

To continue with the Ford dealership example, if the Ford dealership was enrolled in Remarketing, it would have Google code snippets, allowing Google to cookie its visitors. It could then tell Google to show their display ad to all visitors who looked at cars but did not order them or schedule sales appointments, to try to entice those visitors to return. This highly targeted audience could be defined to Google as (the set of inventory page visitors) minus (the set of order confirmation page visitors) minus (the set of appointment confirmation page visitors). Furthermore, the Ford dealership could specify that the content of the display ads be the exact cars that the visitors were looking at. Google can then use the AdSense platform to show an ad containing the specific car a user was looking at to the user wherever they go on millions of AdSense publishing websites, for as long as the dealership wants to keep paying Google to serve them.[37]

The significance of this is that the advertising targeting is now narrowed down to the level of the individual. In 2016, Google began offering the Remarketing capability across devices, as long as the user is logged into Chrome, Gmail, or other Google services. This further enables advertisers to follow target individuals around the web. For example, you could look at a car on the Ford dealership's website on your phone at night, and when you go to a news website on your work computer during lunch the next day, you can see an ad for the exact car you were looking at AdWords.[37]

Users can opt out of being remarketed to by Google, but there are other platforms offering advertisers the same or similar capabilities, like AdBrite and AdRoll.

2.15 | Mobile phone surveillance

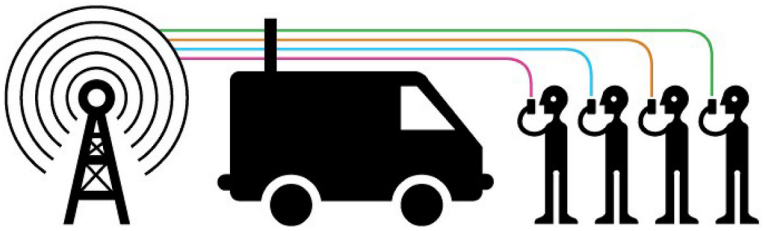
German railways began to develop a wireless telephone in 1918, and by the mid-1920s they were offering the service to first class passengers. Handheld two-way radio transceivers, that is, "walkie talkies," were developed by the US military in the 1940s, albeit in backpack form.

In the same decade, the first automobile-based mobile telephones became available, and by the mid-1960s, demand was greater than what mobile networks could supply, even with technical advances that improved mobile network capacity. In 1973, Motorola produced the first handheld mobile phone. Since then, adoption has been steady, with nearly 300 million users worldwide in 2007.

Prior to fourth generation (4G) mobile technologies, mobile phones connected wirelessly to the same PSTN that landline telephones used, allowing existing switch-based landline surveillance technologies to also monitor mobile calls. Mobile providers began to roll out 4G in 2009, which eliminated circuit switching and instead utilized packet switching on an IP network. This required a technical shift in surveillance techniques as well.

One such technique is to surveil mobile calls wirelessly, and on a more local level, using cell site simulator technology. A cell site simulator is also known as an international mobile subscriber identity (IMSI) catcher or a stingray, the name of one popular model of the device manufactured by the Harris Corporation. Cell site simulators mimic wireless carrier

FIGURE 5 A cell site simulator[41]



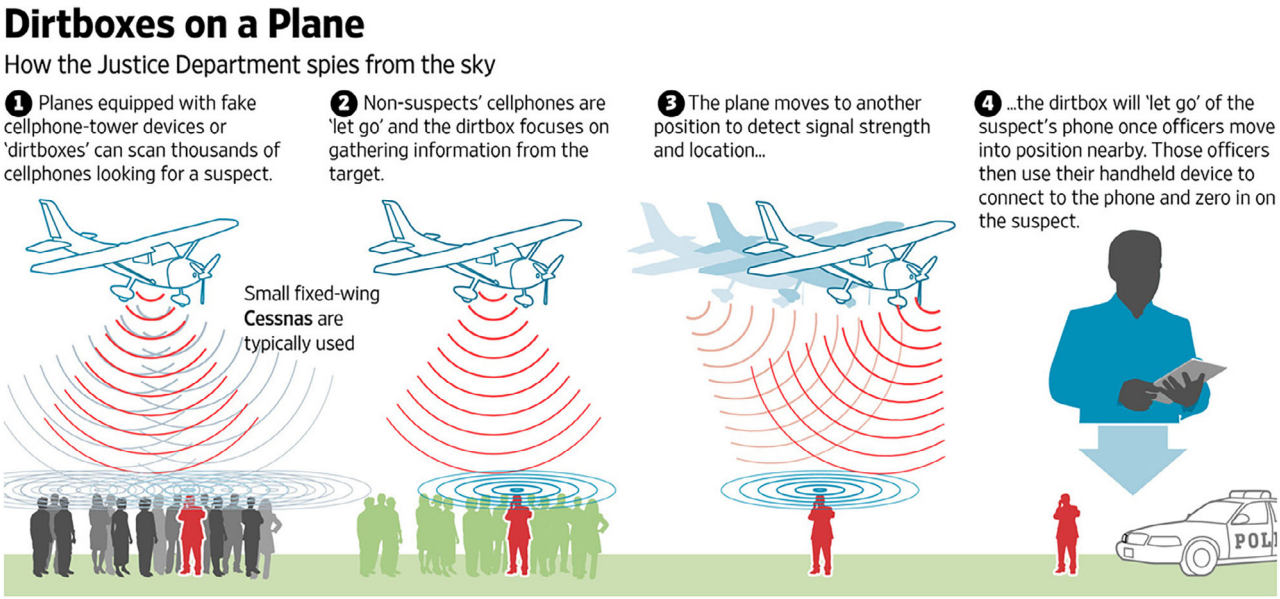


FIGURE 6 Spying from the sky[42]

cell phone towers to trick mobile phones into relaying through them. Using this technique, all mobile data within 200 m or more can be monitored, including device locations, subscriber identification, call contents, text messages, and other data, even allowing the extraction of encryption keys.[38]

Ownership of cell site simulator devices is rarely publicized, but the American Civil Liberties Union has identified its use by state and local police departments in addition to federal agencies.[39] The New York Police Department alone has used the device more than 1000 times since 2008.[40]

One use case of the technology is to locate and operate a cell site simulator at the scene of a civil disturbance as shown in Figure 5. The device could be brought into operational proximity by hand, or by mounting it to a vehicle. The operator would be able to identify individuals in the area, monitor their communications, and degrade or disable their mobile communication ability, if desired, such as by jamming 4G and 3G networks, conducting a denial service attack, or interrupting the relay completely. For example, it was used by the Egyptian government during the Arab Spring uprisings of 2011.

IMSI catcher operations are not limited to terra firma. According to a *Wall Street Journal* report, one law enforcement program deploys IMSI catchers on aircraft to surveil individuals on the ground, as shown in Figure 6.[42] Such deployments can collect data from thousands of mobile phones in a single flight, including each device's IMSI, location data, websites visited, SMS message contents, voice call contents, and call metadata such as the number dialed and length of the call.

2.16 | Satellites

Another modern example of surveillance technology is the use of satellite imagery. For example, multiple municipal offices in the United States have used commercially purchased satellite imagery of residential areas (or images from Google Earth) to identify unlicensed or illegal backyard pools.

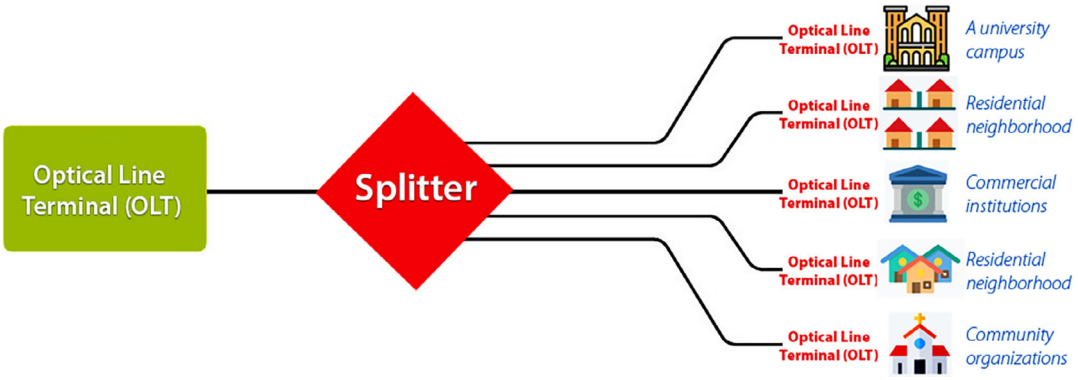


FIGURE 7 A fiber optic splitter

GPS satellites collect location and movement data for compatible and connected devices. Regardless of where one might be on earth, it is likely that between five and eight GPS satellites are above them.

Reconnaissance satellites (sometimes informally known as spy satellites) have been deployed since 1960 to collect a variety of data for military and intelligence purposes. They provide not only early missile warning, troop movement monitoring, and nuclear site detection, but also optical imaging powerful enough to see an individual person. While a US federal regulation limits the resolution of images taken by commercial satellites to 25 cm, reconnaissance satellites can capture images far more granular.

In addition, they can detect movement via infrared light or heat emission, and hear inaudible electronic beeps transmitted by GPS systems. According to a report published in *MIT Technology Review* on 26 June 2019, such satellites will soon be able to watch people everywhere and all the time.

2.17 | Internet surveillance

In 1993, use of the Internet accounted for 1% of data transmitted through worldwide telecommunications networks. By 2007, it had grown to 97%.[43] Internet data are transmitted across much of the same infrastructure used for other forms of telecommunication. Therefore, prior techniques and business relationships could be leveraged to surveil it.

One example is the government installation of fiber optic splitters at major commercial switching stations. In 2006, former AT&T technician Mark Klein detailed the existence of a beam splitter in a dedicated room at an AT&T switching facility in San Francisco. According to Klein, he helped to install the splitter for use by the NSA. Figure 7 illustrates a splitter.

In 2012, former NSA intelligence official William Binney estimated there were 10 to 20 splitters operated by the NSA at major switching stations throughout the United States.[44] Fiber optic splitters make a full copy of everything passing through the line, including all call and Internet data. Therefore, the NSA has direct access to nearly all domestic Internet data, and any international data routed through the same lines.

Deep packet inspection (DPI) is another way that Internet traffic can be surveilled. DPI is a robust form of packet filtering that can inspect network packets at any of the seven layers of the OSI model. The Chinese government uses DPI as one of the key firewall technologies of its Golden Shield Project. Golden Shield is tasked with detecting and blocking any Internet content or use which undermines national unification, contains sexually suggestive content, encourages gambling or violence, and so on. To that end, Golden Shield has DPI firewalls running at all of the Internet gateways serving the country, to inspect packets for specific keywords. For example, a website which is not blocked at the domain level may still have certain pages filtered out due to containing keywords such as blackjack or anarchy.

Running communication cables underwater has been done for over 150 years, since the time of the telegraph. In 1971, the US Navy, CIA, and NSA used a submarine and divers to attach a non-invasive recording device on a cable in the Sea of Okhotsk, to monitor communications between two Soviet bases.

Today, more than a half million miles of fiber optic undersea cables carry Internet and other telecommunication data around the world. They essentially form the backbone of the Internet, connecting countries and continents. Tapping happens at signal amplification points underwater and at terrestrial coastal stations where the cables make landfall. When done at coastal stations, it is usually done with the knowledge and consent of the host country.[45]

All data passing through a tapped cable are captured, including phone calls, emails, social media posts, and more.[46] As of 2013, one British intelligence program called Tempora harvested 21 million gigabytes of data per day from undersea cable taps and kept each day's take for a month for joint analysis with the NSA.[47]

Perhaps even the previously discussed cookie pooling is a form of Internet surveillance because it relies on the HTTP protocol which is most frequently used on the Internet.

2.18 | Cracking encryption

Whether transmitted via airwaves or optical fiber, sensitive data are often encrypted. In fact, roughly half of all web traffic is now encrypted with the HTTPS protocol. So, to be able to surveil such platforms effectively, a method for subverting encryption is required.

Intended recipients in the possession of proper keys can decrypt encrypted messages easily. But unintended recipients must use cryptanalysis, which can be highly time-intensive and labor-intensive, even with the benefit of modern computing. Cryptanalysis is nearly as old as cryptography itself, and the two practices have evolved together. An Arabian named Al-Kindi wrote the first known cryptanalysis manual in the ninth century AD. It could be argued that the need for stronger cryptanalysis in World War II drove the development of the computer itself, producing machines such as Alan Turing's electromechanical Bombe, and Tommy Flowers' Colossus, the first electronic digital computer. Both machines helped to break German encryption and win the war for the west.

Today's encryption requires far more powerful computers to crack, and thus far more powerful supercomputers are being developed for the task. In 2004, the Defense Advanced Research Projects Agency (DARPA) launched the High Productivity Computing Systems program in Oak Ridge, Tennessee, with the goal of creating a computer that could execute one quadrillion operations a second, also known as a petaflop. In 2009, the program announced the achievement of 1.75 petaflops per second with a warehouse sized supercomputer it called Jaguar. At the same time, the NSA developed their own supercomputer alongside the DARPA team, specifically for cryptanalysis. The ciphertext it cryptanalyzes comes from a new $2 billion, million square foot data center in Utah, where the NSA stores the raw data from its fiber optic splitters and other surveillance programs.[44]

Where possible, it is best to avoid the burden of cryptanalysis altogether. One way this is done is by soliciting backdoors from vendors. An even more powerful way is to insert a backdoor directly into an encryption algorithm, such as was done in an encryption standard adopted by the National Institute of Standards and Technology in 2006.[48] A final method of note that the NSA uses is tapping into Google data centers outside of US borders, since SSL is removed there and traffic for Gmail and other Google services is transmitted in the clear.[49] It is not known if Google had knowledge of these efforts before they became publicly known in 2013.

2.19 | Data mining

Data mining is a process by which a large volume of data is mined, that is, searched, processed, correlated, and explored using a variety of statistical, analytical, search, and retrieval algorithms. Tools, techniques, and contexts may vary but the objectives are the same: capturing useful information based on data relationships that were previously hidden but can now be revealed and taken advantage of. Businesses do this to learn more about their customers or for product retailing, marketers do it for deciding on a new product, and governments do it to detect fraud, assess risk, or potentially predict future events. In fact, data mining has become one of the key activities of many homeland security initiatives, as outlined in the CRS Report for Congress.[50]

Data mining is often applied to public and statistical data that were produced long before today's sophisticated search and analytical tools were envisioned. Thus, despite its many benefits and valid applications, data mining also introduces privacy concerns. Sumathi and Sivanandam[51] investigate potentially damaging aspects of collecting and using secondary personal information (ie, data not intended for statistical purposes). Three of their conclusions are as follows:

- The discovered data may include misinformation damaging to individuals or organizations.
- Data discovery may result in granulated access to personal information.
- Overly generalized patterns may be applied to the discovery process, forming damaging stereotypes.

In addition, public data often include a chain of relationship information from which private data may be inferred. A data mining technique that exploits this fact is called an *inference attack*. In an inference attack, a publicly available data set is analyzed to discover private information, where the chance of success increases with the amount of domain knowledge possessed by the analyst. The previously discussed CA case illuminated one such effort conducted with social media data.

3 | ATTRIBUTES AND PREDICTION OF NEXT GENERATION METHODS

Mass surveillance is observation that has been scaled up past some threshold in terms of the number of objects being surveilled, or the size of the surveilled area. It targets all individuals or objects that match a desired set of characteristics. Throughout this paper, we have considered a number of mass surveillance methods. We can now analyze the methods to determine what attributes they express. We propose a set of 18 attributes, which cover various aspects of the methods, such as the nature of what they monitor, how they function, and how they are intended to be used:

1. *Monitoring physical objects*. This attribute considers what is being surveilled. An example of this would be radar's detection of aircraft.
2. *Monitoring people*. An argument could be made that all surveillance comes down to monitoring people in the end. But what is it monitoring directly? A CCTV installation at a football stadium would be an example of monitoring people.
3. *Monitoring transportation*. An ALPR system would be an example of monitoring transportation.
4. *Monitoring communications*. Much can be learned from studying the contents of a population's communications. An example of this would be mobile phone surveillance.
5. *Monitoring a medium that desired objects inhabit*. Rather than monitoring a desired object directly, some methods monitor a medium for signatures of their desired objects. An example of this would be how passive sonar monitors water for sound.
6. *Exploitation of sound*. Some methods rely upon sound for their core mechanism. A gunshot listening microphone would be an example.
7. *Exploitation of the electromagnetic spectrum*. Some methods rely upon measuring or manipulating some portion of the electromagnetic spectrum. Radar would be an example of this.
8. *Public data or data freely shared by the object*. When looking at the data collected by a surveillance method, some methods focus on public data. An example of this is CCTV in a public area.
9. *Private data*. Some methods surveil by way of collecting private data, such as tapping a landline telephone.
10. *Help from third party* (*willing or coerced*). Many methods forgo collecting data themselves, and instead request or require a third party that already has the data to provide it.
11. *For immediate use/analysis*. If the data gathered by a method cannot be stored, or is intended for immediate consumption, it can be said to exhibit this attribute.
12. *For future use if desired*. Some methods record and store immense amounts of data intended for analysis later, rather than immediately.
13. *Auxiliary tool or technology*. This attribute applies to methods which assist surveillance more so than perform the actual surveillance.
14. *Physical tapping*. Some methods rely upon physically and invasively connecting to a communication transmission line.
15. *Exploitation of infrastructure*. Many methods rely upon the natural concentration and funneling points provided by infrastructure to achieve the scaling up required for mass surveillance.
16. *For marketing purposes*. The purpose of a surveillance method is another point of differentiation. A relatively recent purpose is marketing.
17. *Manual method*. Early methods such as the census were necessarily manual.
18. *Technical method*. Beginning in the early 1900s, technological means became the norm as a method of mass surveillance.

Table 1 is a matrix of the mass surveillance methods and attributes. Where a method expresses an attribute, it is marked with a one. The methods are sorted roughly in order of emergence with the oldest method at top. Totals of the columns reveal the popularity of each attribute, which can be easily digested with a pie chart shown in Figure 8A.

TABLE 1 Attributes of select mass surveillance methods

Mass surveillance method	Monitoring physical objects	Monitoring people	Monitoring transportation	Monitoring communications	Monitoring a medium that desired objects inhabit	Exploitation of sound	Exploitation of the electromagnetic spectrum	Public data or data freely shared by the object	Private data	Help from third party (willing or coerced)	For immediate use/analysis	For future use if desired	Auxiliary tool or technology	Physical tapping	Exploitation of infrastructure	For marketing purposes	Manual method	Technical method
Unaided observation from higher ground	1	1	1	0	1	0	0	0	0	0	1	0	0	0	0	0	1	0
Informant networks	0	1	0	0	0	0	0	0	1	1	1	1	0	0	0	0	1	0
Postal mail tracking	1	0	0	1	0	0	1	0	1	1	1	1	0	0	1	0	1	1
Sonar	1	0	1	0	1	1	0	0	0	0	1	0	0	0	0	0	0	1
Radar	1	0	1	0	1	0	1	0	0	0	1	0	0	0	0	0	0	1
Telegraph intercepting	0	0	0	1	1	0	1	0	1	1	1	0	0	1	1	0	0	1
Landline telephone tapping	0	0	0	1	1	0	1	0	1	1	1	1	0	1	1	0	0	1
CCTV	1	1	1	0	0	0	1	1	1	0	1	1	0	0	0	0	0	1
Audio processing software	0	0	0	1	0	1	0	1	1	0	1	1	0	0	0	0	0	1
Image processing software	1	1	1	1	1	0	1	1	0	0	1	1	0	0	1	1	0	1
Making use of public data and shared data	0	0	0	1	0	0	0	1	0	1	1	1	0	0	0	1	1	1
Airwave surveillance	0	0	0	1	1	0	1	1	1	0	1	1	0	0	0	0	0	1
Alternative cameras	1	1	1	0	0	0	1	1	1	0	1	1	0	0	0	0	0	1
User action logging	0	1	0	0	0	0	0	1	0	0	1	1	0	0	0	1	0	1
Cookie pooling	0	1	0	0	0	0	0	1	0	1	1	1	0	0	0	1	0	1
Mobile phone surveillance	0	1	0	1	1	0	1	0	1	1	1	1	0	1	1	0	0	1
Internet surveillance	0	1	0	1	1	0	1	0	1	1	1	1	0	1	1	0	0	1
Cracking encryption	0	0	0	1	0	0	0	0	1	0	1	1	1	0	0	0	0	1
Total	7	9	6	10	9	2	10	8	11	8	18	14	1	4	6	4	4	16

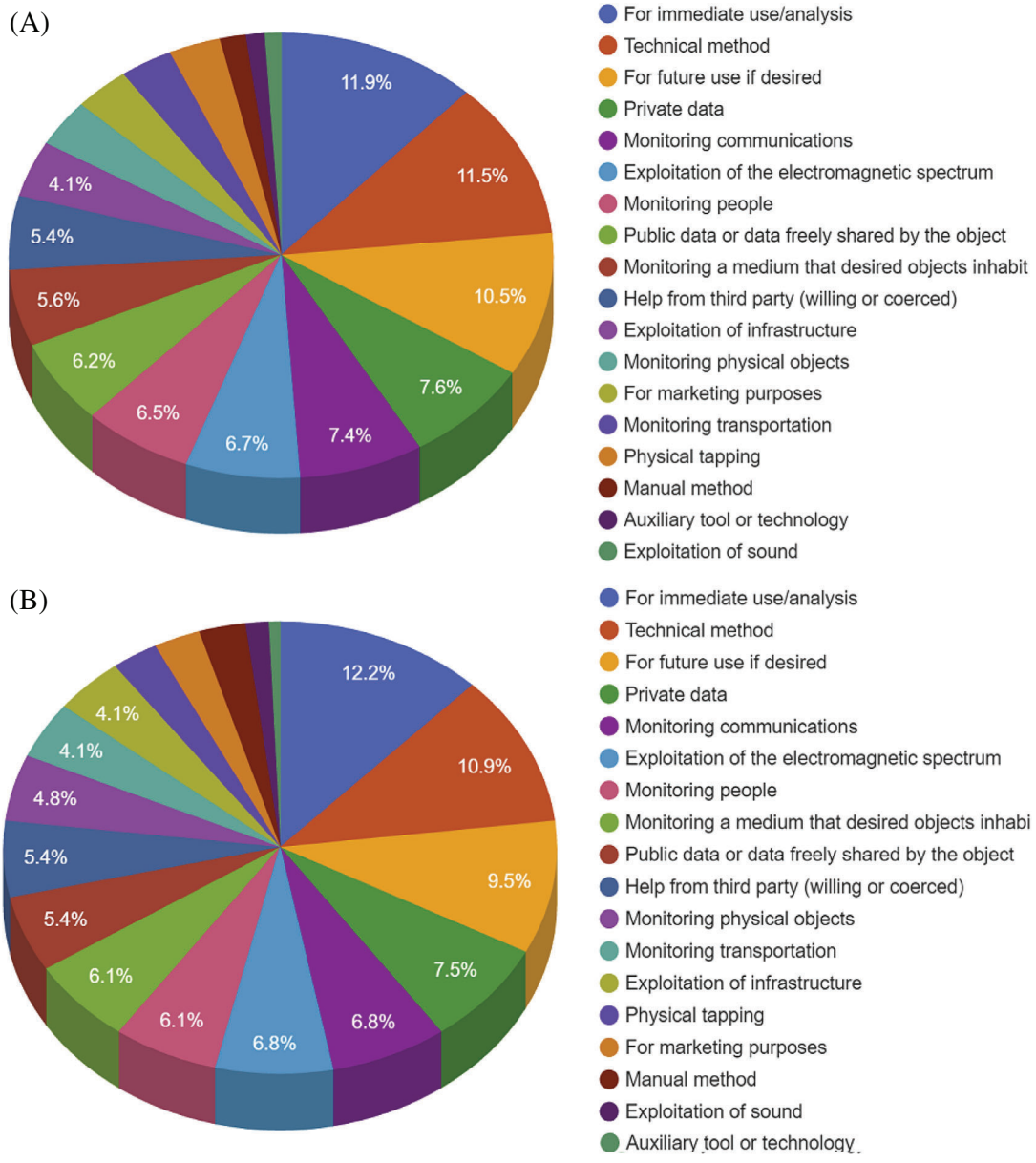


FIGURE 8 A, Frequency of the occurrence of various attributes. B, Recency-weighted frequency of the occurrence of various attributes

All methods expressed the "for immediate use/analysis" attribute, since all data can be analyzed immediately if desired. The next most common attributes in order are:

- *Technical method*. Most methods considered were from the 20th century onward, so this is perhaps not a surprising finding.
- *For future use if desired*. As computing power has increased, the cost of storage has decreased. As a result, surveillance data are often gathered en masse, and later selectively analyzed, such as with a keyword search. This allows analysts to find more later then they could immediately.
- *Private data*. It is common for surveilling actors to pursue private data about the individuals or objects they wish to surveil. The contents of communications are a rich source of private data.
- *Monitoring communications*. Since telecommunications have become so commonly used, and because of the funneling nature of the communications infrastructure, communications have become an irresistible target for those wishing to conduct surveillance.

- *Exploitation of the electromagnetic spectrum*. Much of modern technology exploits the electromagnetic spectrum in some way. For example, visible light enables simple optical cameras, but it also powers the fiber optic cable which makes up the backbone of internet and mobile phone communications.

Next, we added a time-weighting factor to each method, to more heavily weight those that have emerged more recently. This should enhance the predictive power of the model, since future methods are likely to have more in common with more recent methods than with older methods. Table 2 shows the time-weighted factor for each method, which increases linearly in 0.25 increments, beginning at 1 and ending at 5.25. It also shows two columns for each attribute: one with an occurrence tally in the original binary format, and one showing the time-weighted value of each occurrence.

The new weighted totals show that nine of the 18 attributes have changed places in the order (see Figure 7B). However, the first seven places remain the same. Thus, we gain some confidence that our interest in the subset of attributes is warranted.

Next, we abandoned numbers altogether, and presented the data graphically with black and white cells, shown in Table 3, highlighting several patterns of interest that emerged.

Some of the columns are dominated by black, but these are the same columns featured in our first round of analysis. When looking only at the other columns, and by again assuming that more recent occurrences are more likely to be predictive than older occurrences, the "for marketing purposes" and "help from third party (willing or coerced)" columns exhibit patterns of interest. The "for marketing purposes" attribute only started occurring relatively recently, and from the time it started, it has continued to occur with an almost 50% frequency. The "help from third party (willing or coerced)" attribute occurs more consistently recently, including in three out of the four most recent methods.

Overall, we have identified 7 of the 18 attributes as having meaningfully predictive properties. Therefore, a next generation mass surveillance method is likely to exhibit the following characteristics:

- *Technical method*. Following the trend started a century ago, the method will utilize technology in some form.
- *Exploitation of the electromagnetic spectrum*. The technology utilized will use the electromagnetic spectrum for the detection and/or transmission of data.
- *Monitoring communications*. The data surveilled will be a communications platform, such as a popular new social media website or messaging app.
- *Private data*. The surveilled communications will be conversations intended for specific participants rather than public announcements or speeches.
- *Help from third party* (*willing or coerced*). The surveillers will recruit a corporate partner to help. The communication platform owner may be required to share their data, or they may willingly sell it.
- *For future use if desired*. Rather than surveilling a small set of targeted communications, a much larger data set will be collected and stored, and any targeted searching will be performed on the stored data set.
- *For marketing purposes*. There is a roughly 50% chance that the surveillance will be done for marketing purposes. For example, it could be to serve up targeted advertising to the users of the communication platform.

4 | REACTIONS AND IMPLICATIONS IN SOCIETY

Whatever shape next generation mass surveillance methods may take, the way that society responds to them is likely to be like what has occurred in recent years.

New government surveillance programs and capabilities will be kept in secrecy, and only learned about years or even decades later, when disgruntled or conscience-burdened insiders team up with determined journalists. As a result, federal legislation will be passed to place new limits on domestic surveillance practices. This happened when Perry Fellwock revealed the existence of the NSA through Ramparts magazine in 1971, which led to the US Senate Church Committee Hearings, which in turn led to the Foreign Intelligence Surveillance Act of 1975. It also happened when Edward Snowden revealed the extent of modern NSA practices to The Guardian and Washington Post in 2013, which led to the passage of the USA Freedom Act in 2015.

New corporate surveillance practices may be learned about from changes to Terms of Service or Privacy Policy agreements. They are likely to provoke debate in the court of public opinion, and perhaps any number of private lawsuits, but

TABLE 2 Attributes of select mass surveillance methods

Mass surveillance method	Time-weighting factor		Monitoring physical objects		Weighted score	Monitoring people		Weighted score	Monitoring transportation		Weighted score	Monitoring communications		Weighted score	Monitoring a medium that desired objects inhabit		Weighted score	Exploitation of sound		Weighted score	Exploitation of the electromagnetic spectrum		Weighted score	Public data or data freely shared by the object		Weighted score	Private data		Weighted score	Help from third party (willing or coerced)		Weighted score	For immediate use/analysis		Weighted score	For future use if desired		Weighted score	Auxiliary tool or technology		Weighted score	Physical tapping		Weighted score	Exploitation of infrastructure		Weighted score	For marketing purposes		Weighted score	Manual method		Weighted score	Technical method		Weighted score
Unaided observation from higher ground	1.00	1	1.00	1	1.00	1	1.00	0	0.00	1	1.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	1	1.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	1	1.00	0	0.00
Informant networks	1.25	0	0.00	1	1.25	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	1	1.25	1	1.25	1	1.25	1	1.25	0	0.00	0	0.00	0	0.00	0	0.00	1	1.25	0	0.00
Postal mail tracking	1.50	1	1.50	0	0.00	0	0.00	1	1.50	0	0.00	0	0.00	1	1.50	0	0.00	1	1.50	1	1.50	1	1.50	1	1.50	0	0.00	0	0.00	1	1.50	0	0.00	1	1.50	1	1.50
Sonar	1.75	1	1.75	0	0.00	1	1.75	0	0.00	1	1.75	1	1.75	0	0.00	0	0.00	0	0.00	0	0.00	1	1.75	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	1	1.75
Radar	2.00	1	2.00	0	0.00	1	2.00	0	0.00	1	2.00	0	0.00	1	2.00	0	0.00	0	0.00	0	0.00	1	2.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	1	2.00
Telegraph intercepting	2.25	0	0.00	0	0.00	0	0.00	1	2.25	1	2.25	0	0.00	1	2.25	0	0.00	1	2.25	1	2.25	1	2.25	0	0.00	0	0.00	1	2.25	1	2.25	0	0.00	0	0.00	1	2.25
Landline telephone tapping	2.50	0	0.00	0	0.00	0	0.00	1	2.50	1	2.50	0	0.00	1	2.50	0	0.00	1	2.50	1	2.50	1	2.50	1	2.50	0	0.00	1	2.50	1	2.50	0	0.00	0	0.00	1	2.50
CCTV	2.75	1	2.75	1	2.75	1	2.75	0	0.00	0	0.00	0	0.00	1	2.75	1	2.75	1	2.75	0	0.00	1	2.75	1	2.75	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	1	2.75
Audio processing software	3.00	0	0.00	0	0.00	0	0.00	1	3.00	0	0.00	1	3.00	0	0.00	1	3.00	1	3.00	0	0.00	1	3.00	1	3.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	1	3.00
Image processing software	3.25	1	3.25	1	3.25	1	3.25	1	3.25	1	3.25	0	0.00	1	3.25	1	3.25	0	0.00	0	0.00	1	3.25	1	3.25	0	0.00	0	0.00	1	3.25	1	3.25	0	0.00	1	3.25
Making use of public data and shared data	3.50	0	0.00	0	0.00	0	0.00	1	3.50	0	0.00	0	0.00	0	0.00	1	3.50	0	0.00	1	3.50	1	3.50	1	3.50	0	0.00	0	0.00	0	0.00	1	3.50	0	3.50	1	3.50
Airwave surveillance	3.75	0	0.00	0	0.00	0	0.00	1	3.75	1	3.75	0	0.00	1	3.75	1	3.75	1	3.75	0	0.00	1	3.75	1	3.75	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	1	3.75
Alternative cameras	4.00	0	4.00	1	4.00	1	4.00	0	0.00	0	0.00	0	0.00	1	4.00	1	4.00	1	4.00	0	0.00	1	4.00	1	4.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	1	4.00
User action logging	4.25	0	0.00	1	4.25	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	1	4.25	0	0.00	0	0.00	0	4.25	1	4.25	0	0.00	0	0.00	0	0.00	1	4.25	0	0.00	1	4.25
Cookie pooling	4.50	0	0.00	1	4.50	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	1	4.50	0	0.00	1	4.50	1	4.50	1	4.50	0	0.00	0	0.00	0	0.00	1	4.50	0	0.00	1	4.50
Mobile phone surveillance	4.75	0	0.00	1	4.75	0	0.00	1	4.75	1	4.75	0	0.00	1	4.75	0	0.00	1	4.75	1	4.75	1	4.75	1	4.75	0	0.00	1	4.75	1	4.75	0	0.00	0	0.00	1	4.75
Internet surveillance	5.00	0	0.00	1	5.00	0	0.00	1	5.00	1	5.00	0	0.00	1	5.00	0	0.00	1	5.00	1	5.00	1	5.00	1	5.00	0	0.00	1	5.00	1	5.00	0	0.00	0	0.00	1	5.00
Cracking encryption	5.25	0	0.00	0	0.00	0	0.00	1	5.25	0	0.00	0	0.00	0	0.00	0	0.00	1	5.25	0	0.00	1	5.25	1	5.25	1	5.25	0	0.00	0	0.00	0	0.00	0	0.00	1	5.25
Totals	*n/a*	7	16.25	9	30.75	6	14.75	10	34.75	9	26.25	2	4.75	10	31.75	8	29.00	11	36.00	8	25.25	18	56.25	14	49.25	1	5.25	4	14.50	6	19.25	4	15.50	4	7.25	16	54.00

TABLE 3 Graphical view of the simple binary data set

they are less likely to lead to legislation. Nevertheless, some concessions may be gained due to the corporate need for good public relations. For example, the social media website Instagram updated its terms in 2012 to specify increased sharing of user data to allow for the incorporation of targeted advertisements. But when public concern emerged that the new terms would result in the selling of user photographs, Instagram reverted portions of the terms back to an earlier version.

Public debate will take place through our surrogates in the news media and entertainment media. Through an informal agenda-setting process, media outlets tend to coalesce around similar stories, such as how the content of evening television news programs has been found to be influenced by the content of the morning New York Times.[52] In 2013, The New York Times published 620 articles that contained the word Snowden,[53] and coverage of NSA programs and ruminations on privacy issues dominated news media across the United States. Time magazine declared it the top news story of 2013.[54]

The public will also make its voice heard more directly using social media. Many social media platforms allow users to employ the use of hashtags, which are custom content-tagging keywords that can be easily searched, such as #Snowden. Any user can create a hashtag, any user can search for all posts containing a given hashtag, and the platforms themselves

often encourage hashtag use by promoting or highlighting the hashtags that they identify as currently trending. As a result, users are able to create and participate in their own online publications, centered around their specific conversations of interest, limited only by the size of the platform's user base. Twitter has 319 million users today[55]; Facebook has almost two billion.[56]

Social media use has become so popular today that public conversations on social media are often used as source material for more traditional forms of media. According to a 2013 study in the journal *Journalism Practice*, Twitter "tweets" are being increasingly included as quotes in newspaper reporting.[57] In doing so, traditional media is granting a degree of official acceptance and importance to social media platforms, perhaps further precipitating their rise.

Interestingly with regard to surveillance issues, the tone of writing tends to vary between traditional news media and social media conversations, with social media conversations tending to show a greater degree of disfavor for mass surveillance practices. For example, a 2015 semantic network analysis study found that social media users associated Edward Snowden with "other whistle-blowers, bipartisan issues, and personal privacy issues, while professional journalists associated the Snowden incident with issues of national security and international relations."[58] This is perhaps not surprising given that traditional news media organizations have more stakeholders to please, including corporate management, shareholders, advertisers, and government regulators, which results in a more measured approach than an unaffiliated individual can take on social media.

In addition to media coverage, social media engagement, and possible legislation, several other societal reactions can be expected when a new mass surveillance method is publicly revealed. There will be a chilling effect for a period on personally sensitive and government-sensitive topics on the platform for which the surveillance is revealed. This self-censoring behavior was observed in Google search use following the 2013 revelation of the worldwide internet surveillance capabilities of the NSA.[59] There will be a rise in the adoption of encryption technologies such as HTTPS,[60] however the rise will mostly be attributable to the actions of manufacturers rather than end users. The end users themselves, that is, the public, are likely to have a "limited and short-lived" interest in the personal use of encryption or other privacy-enhancing behaviors, as was observed after the 2013 revelations.[61]

5 | SURVEILLANCE, EXPLOSION OF TECHNOLOGY, AND IMPACT ON PRIVACY

Rapid technological developments have increasingly enhanced traditional and modern surveillance devices. These technologies are used by governments, corporations, and individuals alike for "focused, systematic and routine attention to personal details for purposes of influence, management, protection or direction."[62] According to IBM, the information big bang and explosion of technology has led to the creation of two quintillion* bytes of data on a daily basis. Such a sheer and relentlessly growing volume of data complicates matters for those conducting surveillance, and for privacy advocates.

Privacy is intrinsically intertwined with surveillance, because any time a form of surveillance is employed by advertisers, pollsters, retailers, or government, some form of an individual' privacy may be impacted. One common concern is that today's surveillance technologies overreach. For example, former Secretary General of the UN Ban Ki-moon stated, "I am disturbed by how states abuse laws on internet access. I am concerned that surveillance programmes are becoming too aggressive."[63]

Others counter that it is the very reach and scope of modern implementations that drive improvements in surveillance efficacy, and the technological benefits to society that follow. For example, without the continued development and widespread use of radar after World War II, we would not have collision avoidance systems in vehicles today.

But there also exist more nuanced opinions, such as that mass surveillance carries both risk and rewards, and that with careful deliberation, we can maximize utility while limiting harm. Ban Ki-moon hints at an openness to this approach in the same speech as his comment above: "I understand that national security and criminal activity may justify some exceptional and narrowly-tailored use of surveillance. But that is all the more reason to safeguard human rights and fundamental freedoms."[63]

Indeed, the deliberation to determine the appropriate balance between surveillance utility and personal privacy has been ongoing for some time within academia, industry professional associations, legislative branches of government, and the court of public opinion. While the media wields agenda setting power and industry holds great political influence, legislatures are often the final arbiters, as evidenced by the recent passage of bills like the California Consumer Privacy Act and the European Union's General Data Protection Regulation. Countries in Asia and Africa have adopted similar guidelines for the collection, storing and control of an individual's data.

Such rule-making procedures are often slow by design to encourage long term thinking and hopefully produce consensus between stakeholders. In the meantime, individuals have access to advanced technologies for securing data.

6 | CONCLUSIONS

We seem to be hardwired as a species to feel the need to surveil, and to seek out information about the world around us. And indeed, we are not the only species with such a need.[64] As such, there has always been surveillance in society. Thousands of years ago, mass surveillance was limited by primitive technology, however higher ground observations and census decrees did provide an advantage. Today, mass surveillance is more prevalent simply because advancing technology has increased the number of methods by which we can accomplish it. If Augustus Caesar had the ability to analyze the private conversations of Rome's citizens and subjects, it is hard to believe that he would have eschewed its use.

Technology will continue to advance in the future, and the methods of mass surveillance will continue to advance in concert. By analyzing the attributes of past and current methods, we can make educated guesses about what attributes next generation methods are likely to exhibit. We are likely to see new communication-monitoring methods which employ third-party assistance to collect large amounts of private communication data for future analysis.

How best to react to such methods, or how to adjudicate for them in advance are questions worth careful deliberation. The answers will determine the risk-reward balance for mass surveillance programs, and in doing so, reveal our priorities.

6.1 | Future research

Our introduction and prediction of the attributes of future surveillance technologies were based on our comprehensive studies of past and present technologies. As stated, they are predicted attributes. Additional research is needed to fully investigate and refine these attributes. Software simulation and experimentation will help evaluate their characteristics and validate their importance.

Surveillance and privacy are inextricably linked. Thus, broad coalitions of government officials, technology experts, business leaders, consumer advocates, and legal scholars will need to collaborate to develop frameworks which allow us to reap utility from surveillance technologies while minimizing harm.

ENDNOTE

*One with 30 zeros.

ORCID


Hossein Saiedian https://orcid.org/0000-0001-5060-6332

REFERENCES

1. Rosenberg M, Goldman A, Huetteman E. Monitoring may have 'incidentally' picked up Trump aides, House Member says. *The New York Times*, 2017. https://www.nytimes.com/2017/03/22/us/politics/devin-nunes-wiretapping-trump.html?_r=0. Accessed January 13, 2021.
2. Miller G, Nakashima E. WikiLeaks says it has obtained trove of CIA hacking tools. *The Washington Post*, 2017. https://wapo.st/3a9lgNs. Accessed January 13, 2021.
3. Solon O. US border agents are doing 'digital strip searches'. Here's how to protect yourself. *The Guardian*, 2017. https://bit.ly/3accZZc. Accessed January 13, 2021.
4. Brodkin J. Senate votes to let ISPs sell your web browsing history to advertisers. *Ars Technica*. Conde Nast, 2017. https://arstechnica.com/tech-policy/2017/03/senate-votes-to-let-isps-sell-your-web-browsing-history-to-advertisers. Accessed January 13, 2021.
5. Rosenbach M, Stark H, Stock J. Data surveillance with global implications. *Spiegel Online*, 2013. http://www.spiegel.de/international/world/prism-leak-inside-the-controversial-us-data-surveillance-program-a-904761.html. Accessed January 13, 2021.
6. Gray D, Henderson S. The Cambridge handbook of surveillance law. *Cambridge Law Handbooks*. Cambridge University Press; 2019.
7. Ucak H. Law enforcement intelligence recruiting confidential informants within "religion-abusing terrorist networks". *VCU Scholars Compass*. Virginia Commonwealth University, 2012. https://scholarscompass.vcu.edu/cgi/viewcontent.cgi?article=3716&context=etd. Accessed January 13, 2021.
8. Bloom RM. *Ratting: The Use and Abuse of Informants in the American Justice System*. Praeger Publishers; 2002. https://www.semanticscholar.org/paper/Ratting%3A-The-Use-and-Abuse-of-Informants-in-the-Bloom/6bd4050b2a71081fc702f1260a5098e277d98cab. Accessed January 13, 2021.
9. If You See Something, Say Something, Official Website of the Department of Homeland Security. https://www.dhs.gov/see-something-say-something and https://www.dhs.gov/see-something-say-something/campaign-materials. Accessed January 13, 2021.

10. McCurdy E. *Leonardo da Vinci's Note-Books: Arranged and Rendered into English with Introductions*. Empire State Book Company; 1923:66.
11. https://en.wikipedia.org/wiki/Sonar. Accessed October 20, 2020.
12. Long D. CBP's Eyes in the Sky. Official Website of the Department of Homeland Security, 2017. https://www.cbp.gov/frontline/frontline-november-aerostats. Accessed January 13, 2021.
13. https://en.wikipedia.org/wiki/JLENS. Accessed October 20, 2020.
14. Budiansky S. *Code Warriors*. Alfred A. Knopf; 2016:286-291.
15. USPTO. United States Patent 5,590,171, USPTO Patent Full-Text and Image Database, 1996. https://bit.ly/30GyrlM. Accessed January 13, 2021.
16. Mannoni L. *Light and Movement: Incunabula of the Motion Picture*. British Film Institute Publishing; 1995:1420–1896.
17. Yesil B. Watching Ourselves: Video surveillance, urban space and self-responsibilization. *Cultural Studies*. 2006;20(4-5):400–416.
18. Walsh BC, Farrington DP. Public area CCTV and crime prevention: an updated systematic review and meta-analysis. *Justice Quart*. 2009;26:716-745. https://doi.org/10.1080/07418820802506206.
19. Keenan TP. *Technocreep: The Surrender of Privacy and the Capitalization of Intimacy*. Greystone Books; 2014:28.
20. Lewis P. You're being watched: there's one CCTV camera for every 32 people in UK. *The Guardian*. Guardian News and Media Limited, 2011. https://www.theguardian.com/uk/2011/mar/02/cctv-cameras-watching-surveillance. Accessed January 13, 2021.
21. Froomkin D. The computers are listening: how the NSA converts spoken words into searchable text. *The Intercept*. First Look Media, 2005. https://theintercept.com/2015/05/05/nsa-speech-recognition-snowden-searchable-text. Accessed January 13, 2021.
22. Pontin MW. Better face recognition software: computers outperform humans at recognizing faces in recent tests. *MIT Technology Review*, 2007. https://www.technologyreview.com/s/407976/better-face-recognition-software. Accessed January 13, 2021.
23. Constine J. Like by smiling? Facebook acquires emotion detection startup FacioMetrics. *TechCrunch*. AOL Inc, 2016. https://techcrunch.com/2016/11/16/facial-gesture-controls. Accessed January 13, 2021.
24. Giles J. Cameras know you by your walk. *New Scientist*. Reed Business Information Ltd, 2012. https://www.newscientist.com/article/mg21528835-600-cameras-know-you-by-your-walk. Accessed January 13, 2021.
25. Wang W, Liu AX, Shahzad M. Gait recognition using WIFI signals. *UbiComp2016. Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing*; 2016:363-373. http://dl.acm.org/citation.cfm?id=2971670. Accessed January 13, 2021.
26. Farivar C. NYPD to conduct "virtual stakeouts," get alerts on wanted cars nationwide. *Ars Technica*. Conde Nast, 2015. https://arstechnica.com/tech-policy/2015/03/nypd-to-conduct-virtual-stakeouts-get-alerts-on-wanted-cars-nationwide. Accessed January 13, 2021.
27. Sellers FS. Cruz campaign paid $750,000 to 'psychographic profiling' company. *The Washington Post*. WP Company LLC, 2015. https://www.washingtonpost.com/politics/cruz-campaign-paid-750000-to-psychographic-profiling-company/2015/10/19/6c83e508-743f-11e5-9cbb-790369643cf9_story.html?utm_term=.084319c707c9. Accessed January 13, 2021.
28. CA. *The Cambridge Analytica Files*. The Guardian; 2017. https://www.theguardian.com/news/series/cambridge-analytica-files. Accessed January 13, 2021.
29. Davies H. Ted Cruz using firm that harvested data on millions of unwitting Facebook users, *The Guardian*. Guardian News and Media Limited, 2015. https://www.theguardian.com/us-news/2015/dec/11/senator-ted-cruz-president-campaign-facebook-user-data. Accessed January 13, 2021.
30. Biesecker M, Bykowicz J. *Cruz App Data Collection Helps Campaign Read Minds of voters*. AP. Associated Press; 2016. https://apnews.com/article/2db0fc93cf664a63909e26e708e91c67. Accessed January 13, 2021.
31. RAF. RAF Menwith Hill – primary mission. Royal Air Force Website. *UK Crown*, 2017. http://www.raf.mod.uk/organisation/rafmenwithhillmission.cfm. Accessed January 13, 2021.
32. Norton-Taylor R. Menwith Hill eavesdropping base undergoes massive expansion. *The Guardian*. Guardian News and Media Limited, 2012. https://www.theguardian.com/world/2012/mar/01/menwith-hill-eavesdropping-base-expansion. Accessed January 13, 2021.
33. https://en.wikipedia.org/wiki/HTTP/_cookie. Accessed October 20, 2020.
34. EU. Cookies, Information Providers Guide: The EU Internet Handbook. European Commission, 2020. http://ec.europa.eu/ipg/basics/legal/cookies/index/_en.htm. Accessed January 13, 2021.
35. Geary J. DoubleClick (Google): What is it and what does it do? *The Guardian*. 2012. https://www.theguardian.com/technology/2012/apr/23/doubleclick-tracking-trackers-cookies-web-monitoring. Accessed January 13, 2021.
36. AdSense. *About Google Ads, AdSense Help*. Google Inc; 2020. https://support.google.com/adsense/troubleshooter/1631343. Accessed January 13, 2021.
37. Remarketing. About Remarketing. *AdWords Help*. Google Inc, 2017. https://support.google.com/adwords/answer/2453998?hl=en. Accessed January 13, 2021.
38. Biddle S. Long-secret stingray manuals detail how police can spy on phones. *The Intercept*. First Look Media, 2016. https://theintercept.com/2016/09/12/long-secret-stingray-manuals-detail-how-police-can-spy-on-phones/. Accessed January 13, 2021.
39. Stingray tracking devices: who's got them? ACLU Website. American Civil Liberties Union. https://www.aclu.org/map/stingray-tracking-devices-whos-got-them. Accessed January 13, 2021.
40. NYCLU. NYPD has used Stingrays more than 1,000 Times Since 2008. NYCLU Website. American Civil Liberties Union of New York, 2016. https://www.nyclu.org/en/press-releases/nypd-has-used-stingrays-more-1000-times-2008. Accessed January 13, 2021.
41. Falcon E. *FCC Helped Create the Stingray Problem, Now it Needs to Fix It, Electronic Frontier Foundation Website*. Electronic Frontier Foundation; 2016. https://www.eff.org/deeplinks/2016/08/fcc-created-stingray-problem-now-it-needs-fix-it. Accessed January 13, 2021.
42. Hruska J. Justice Department to review use of stingrays, other surveillance equipment, May 4, 2015. https://www.extremetech.com/computing/204887-justice-department-will-review-use-of-stingrays-other-surveillance-equipment. Accessed November 25, 2020.

43. Hilbert M, Lopez P. The world's technological capacity to store, communicate, and compute information. *Science*. 2011;332:60-65.
44. Bamford J. The NSA is building the country's biggest spy center (watch what you say). *Wired*, 2012. https://www.wired.com/2012/03/ff-nsadatacenter/. Accessed January 13, 2021.
45. Khazan O (2013). The creepy, long-standing practice of undersea cable tapping. *The Atlantic*. The Atlantic Monthly Group, 2013. https://www.theatlantic.com/international/archive/2013/07/the-creepy-long-standing-practice-of-ndersea-cable-tapping/277855. Accessed January 13, 2021.
46. MacAskill E, Borger J, Hopkins N, Davies N, Ball J. GCHQ taps fibre-optic cables for secret access to world's communications. *The Guardian*, 2013. https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa. Accessed January 13, 2021.
47. Marks P. Submarine internet cables are a gift for spooks. *New Scientist*. Reed Business Information Ltd, 2013. https://www.newscientist.com/article/dn23752-submarine-internet-cables-are-a-gift-for-spooks/\LY1\textbackslash#.UeQp7D54aJM. Accessed January 13, 2021.
48. Perlroth N, Larson J, Shane S. N.S.A. able to foil basic safeguards of privacy on web. *The New York Times*, 2013. https://nyti.ms/2DB52Rp. Accessed January 13, 2021.
49. Gellman B, Soltani A. NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say, The Washington Post. WP Company LLC, 2013. https://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html?utm_term=.18f1b4fb1b93. Accessed January 13, 2021.
50. CRS Report for Congress: Data Mining and Homeland Security: An Overview. https://fas.org/sgp/crs/intel/RL31798.pdf. Accessed January 18, 2007.
51. Sumathi S, Sivanandam S. Chapter 12: major and privacy issues in data mining and knowledge discovery. *Introduction to Data Mining and Its Application*. Springer; 2006:271-291.
52. Golan G. Inter-media agenda setting and global news coverage. *Journal Stud*. 2007;7:323-333. https://doi.org/10.1080/14616700500533643.
53. Search Results. *The New York Times*. The New York Times Company. https://nyti.ms/3gH0zLq. Accessed January 13, 2021.
54. Time Staff. Top 10 U.S. News Stories, *Time*. Time, Inc, 2013. http://nation.time.com/2013/12/04/top-10-best-u-s-news-stories. Accessed January 13, 2021.
55. Frommer D, Wagner K. Twitter only grew by two million users during Trump mania — Facebook grew by 72 million. *Recode*. Vox Media, Inc, 2017. https://www.recode.net/2017/2/9/14558890/trump-twitter-user-growth. Accessed January 13, 2021.
56. https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide. Accessed January 13, 2021.
57. Broersma M, Graham T. Twitter as a news source. *Journal Pract*. 2013. https://doi.org/10.1080/17512786.2013.802481.
58. Qin J. Hero on twitter, traitor on news. *Int J Press Polit*. 2015. https://doi.org/10.1177/1940161214566709.
59. Marthews A, Tucker C. Government Surveillance and Internet Search Behavior, *SSRN. RELX Group*, 2017. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2412564. Accessed January 13, 2021.
60. Google. HTTPS at Google, Google Transparency Report. *Google Inc*. 2017. https://www.google.com/transparencyreport/https. Accessed January 13, 2021.
61. Preibusch S. Privacy behaviors after Snowden. *Commun ACM*. 2015;8(5):48-55.
62. Lyon D. *Surveillance Studies: An Overview*. Cambridge: Polity Press; 2007.
63. Ban Ki-moon, Video message to the fourth Annual Freedom Online Coalition Conference: Free and Secure Internet for All, April 28–29, 2014. https://www.un.org/sg/en/content/sg/statement/2014-04-29/secretary-generals-video-message-fourth-annual-freedom-online. Accessed October 2020.
64. Shoemaker PJ. Hardwired for news: using biological and cultural evolution to explain the surveillance function. *J Commun*. 1996. https://bit.ly/33HRkH3. Accessed January 13, 2021.

How to cite this article: Underwood B, Saiedian H. Mass surveillance: A study of past practices and technologies to predict future directions. *Security and Privacy*. 2021;4:e142. https://doi.org/10.1002/spy2.142