The State of Surveillance

A Case Study on the Present and Future of Government Surveillance

August Valera

Abstract.
The methods and applications of surveillance are constantly changing, and in this technological age, are changing faster than ever before. This article examines modern day surveillance, comparing real agencies such as the NSA and TSA to the fictional Thought Police from George Orwell's *1984*. It then goes on to analyze how the private sector and emerging technologies will affect the evolution of government surveillance.

We live in a state of surveillance. Of that, there is no doubt. However, it is not enough to attack surveillance as an invasion of privacy and be done with it. There are downsides and benefits of a surveillance state. And as citizens of a democratic state, the government's decision to surveil its citizens is by delegation a decision we the people made. This article's goal is to outline potential abuses and downfalls of surveillance, and the role that emerging technology will play on its future. By the end of this analysis, the reader should have a general understanding of how a dystopian future can be created, and through that, how it can be avoided.

Big Brother's Watching You (417)

On the subject of totalitarian dystopias, one cannot ignore George Orwell's contribution in *Nineteen Eighty-four*.[1] You would be hard-pressed to find an instance of government oversight without the accompanying reaction of this being the "new Big Brother". However, it is interesting to note is that "...the surveillance capabilities that are now available to governments and corporations dwarf that which Big Brother had access to."[2] Not only that, in many cases, the technology is both readily available in industry but also universally distributed. Take, for instance, the fictional Thought Police's telescreens that watch everyone 24/7, and can even address individuals in order to give them instructions. In our modern world, the Xbox Kinect was viewed as a revolutionary breakthrough in its ability to track players and allow them to affect the game without analog controllers. The new version of the Kinect for the Xbox One, to be released in the near future, is said to have even more features, including improved facial recognition and an infrared sensor, which "...can be most easily compared to how sonar works." Rival consoles,

[1] George, Orwell. *1984*. *Secker and Warburg* (1949).
[2] Taylor, James Stacey. "In Praise of Big Brother: Why We Should Learn to Stop Worrying and Love Government Surveillance." *Public Affairs Quarterly* 19.3 (2005): 227-246.

such as the Playstation 4, have followed suit in developing this technology.[3] The Xbox One also has Skype integration, allowing up to 4 people to chat with each other at the same time.

This device greatly surpasses what the Thought Police could accomplish with their limited telescreens. Understandably, our technology has progressed in ways Orwell would not have been able to predict. However, all the tools are still there for the government to use. Which calls the question, what caused his prediction to fall short? Well, for one, Orwell predicted a world split into three factions constantly at war. This was understandable, seeing how he wrote the book in 1948, right after WWII. We live somewhat differently; the increasing global interdependence has made war between the major world powers virtually impossible. Orwell's society reveled in war, and made it the primary focus justifying government intrusion. America happens to be at "war" right now, but technically, we haven't declared war since World War II, and news of the war rarely appears on the news. However, we have replaced the conventional meaning of war and applied it to almost any problem, such as the "War on Drugs" and the "War on Terror". And warfare itself become less defined, as we start combating multinational groups with no clear means of identification, and take "precautionary" measures against our own "allies" that might have once been considered warfare. So in some sense, Orwell's prediction of society getting used to and desensitized to war has indeed come true, but on the contrary, warfare hasn't become the central focus of society either.

It is highly unlikely that the complete Orwellian prediction will be fulfilled for several reasons. For one, America has a well established foundation of democracy that is intentionally difficult to modify or overthrow. Certain rights that were not present in Ingsoc's time are explicitly laid out within that document, preventing the Thought Police from ever taking root in our government. But just because certain elements of his novel are unlikely, is not to dismiss the argument in its whole. Mentioned later are some of the ways Big Brother could somewhat manifest in reality. But for this section, we will discuss the ethical dilemma of whether Big Brother is a feasible and ethically sound political system to even have. For the sake of this argument, we take "Big Brother" to mean the logistics and technology of Ingsocian society, disjoined from the ideals and practices the Party implemented alongside that. The fundamental question would be more along the lines of "Should a government place its citizens under surveillance, and if so, to what extent?" Of course, there are many frameworks in which to judge this, some more straightforward than others. However, to stick strictly to libertarian or authoritarian would defeat the purpose of having the argument, so we will abstain from that and focus more on the rights and utilitarian approach.

In his article "In Praise of Big Brother", James Stacey Taylor takes the easy way out by ignoring the possibility of institutionalized abuse of surveillance, with the disclaimer:

> The consequentialist proponent of constant and universal State surveillance need not be unduly concerned about the possibility of major abuses of the State surveillance system. If the State were prone to abuse its citizens in this way prior to the installation of such a system, this would provide good consequentialist grounds for resisting its introduction. The consequentialist proponent of constant State surveillance is thus only

[3] "Xbox One vs. Playstation 4: Kinect 2.0 vs. Playstation 4 ... - IGN.com." 2013. 25 Nov. 2013 <http://www.ign.com/blogs/finalverdict/2013/11/02/xbox-one-vs-playstation-4-kinect-20-vs-playstation-4-camera>

> concerned with defending the introduction of such a surveillance system in those cases where the State was not prone to abusing its citizens in this way.[4]

This article is still useful in listing the benefits of a complete surveillance society. Focused mainly on the courtroom, advantages such as objective evidence, equalization of legal counsel between the rich and the poor, and the decrease in overall crime rates cannot be simply written off due to the potential for abuse. But the chance of private information being leaked to the general public, private industry that could profit from it, or outside forces is just as real. Both of these arguments are somewhat true, but rely on fallacy of attacking the premise. Taylor's argument relies on complete universal surveillance, something that isn't currently feasible due to economic restrictions, and will never be possible due to the ideas of Alfred Korzybski,[5] mentioned later in this article. And attacks against his work assume the opposite, that the existence of these universal surveillance means that abuse is inevitable, and the only prevention would be to never implement it.[6]

Living in a Surveillance State (451)

Going back to the topic of Big Brother, Orwell utilizes verbal irony to show the flaws in the Ingsocian government. The theory of doublespeak promotes a society of denying responsibility and encouraging paradoxes in ideology to fit the whims of the Party at the time. These contradictions extend to the naming schema of the government itself: the Ministry of Peace being in charge of war, the Ministry of Love in charge of torturing thought-criminals, etc.[7] In the same way, it is also ironic that two of our real branches of government, ones most known for invading citizens' privacy, are named just as innocuously: the National Security Agency under the Department of Defence, and the Transportation Security Administration under the Department of Homeland Security. Now, this by itself is but an unfortunate coincidence, and would be hailed by critics as an attack on a straw man, if only the similarities ended there. Unfortunately, they don't. It cannot be denied, although the government has tried to on several occasions, that we live in a surveillance state. The TSA and the NSA are just the tip of the iceberg, and there are undoubtedly many more organizations, within our government and the governments of countries around the world, that are watching every move we do. However, the TSA and the NSA are organizations we know quite a bit more about than these unspoken agencies, for obvious reasons, in addition to recent scandals that have occurred within the past few years. This is the reasoning for focusing on these specific agencies in particular, noting that it is only a representation of the whole, and certainly not the very worst government surveillance can get. It is simply the worst that our government's surveillance gets as we know of now.

On paper, the Transportation Security Administration's (TSA) mission is to "Protect the Nation's transportation systems to ensure freedom of movement for people and commerce."[8] The

---

[4] Taylor, James Stacey. "In Praise of Big Brother" (see footnote #2)

[5] Korzybski, Alfred. *Science and sanity: An introduction to non-Aristotelian systems and general semantics*. Institute of GS, 1958.

[6] Stanley, J. "Bigger Monster, Weaker Chains, The Growth of an American." 2003. <http://www.aclu.org/files/FilesPDFs/aclu_report_bigger_monster_weaker_chains.pdf>

[7] Orwell, George. *1984*. (see footnote #1)

[8] Transportation Security Administration. "About TSA | Transportation Security Administration." 2012. 25 Nov.

countless Americans that have been pulled aside for secondary screening would beg to differ exactly how much freedom of movement they have gained from it. It doesn't help that over the past 12 years of its existence, it has failed to catch a single terrorist.[9] Although the majority of the TSA's public work is done in the screening process, and there is plenty of controversy on the effectiveness of those actions, the real issue, and the one we will be talking about in this essay, occurs behind the scenes. Since the TSA's inception, the agency has maintained a secret list of people to bar from flying within the United States. Called the no-fly list, it is infamous for being both extremely unforgiving and in many cases, outright wrong. Take the case of U.S. Senator Edward Kennedy, whose name was used as an alias for a terrorist suspect. Even a recognizable public official, with plenty of identity verification, was denied a boarding pass due to this system. "The TSA has been working on a system for screening airline passengers that it says will improve the no-fly list. But the plan has been delayed by technological challenges and privacy concerns and the agency has not said when it will be ready."[10] In this case, the TSA is acting as an enabler for other government organizations to surveil citizens as a form of risk assessment. For now, that surveillance is limited to a small list of people thought to be of high-risk. That may not always be the case. Presently, there is a voluntary TSA program called Pre ✓ (Pre-check) offering shorter lines and less invasive screening in exchange for a more in-depth background check before your boarding pass is even printed out. This is a pretty good, if somewhat creepy, deal to make, and a small subset has been quick to jump on board with this program. For this subset, the surveillance nightmare has already begun.

> TSA will assess the level of scrutiny that should be applied to passengers based in part on information it draws from various databases. Though the precise information the agency will rely on hasn't been disclosed, the New York Times notes that sources may include car registration and employment data, as well as a passenger's 'tax identification number, past travel itineraries, property records, physical characteristics and law enforcement or intelligence information.'[11]

Taken at face value, this seems like a good idea: an opt-in system which guarantees that the general public is not being actively surveilled, while allowing good, honest layfolk to get screened less and to their terminals faster. It would be technologically superior, and probably save the government money it would have used to screen all those people thoroughly. Most likely, the majority of people flying would eventually give their consent, especially business people and those who have to fly often. However, this would lead to a large group of people under extra surveillance, and a small group of people who retained their privacy, and as a result, are inspected more thoroughly, and probably suspected because of it. And not only by the TSA agents, but by their fellow flyers as well. Now, this sounds more like coercion than a friendly opt-in system. Better to not take the plane at all than to be suspected of being a terrorists. There's always Amtrak, but it would only take one reasonably sized train bomb to have the TSA start

---

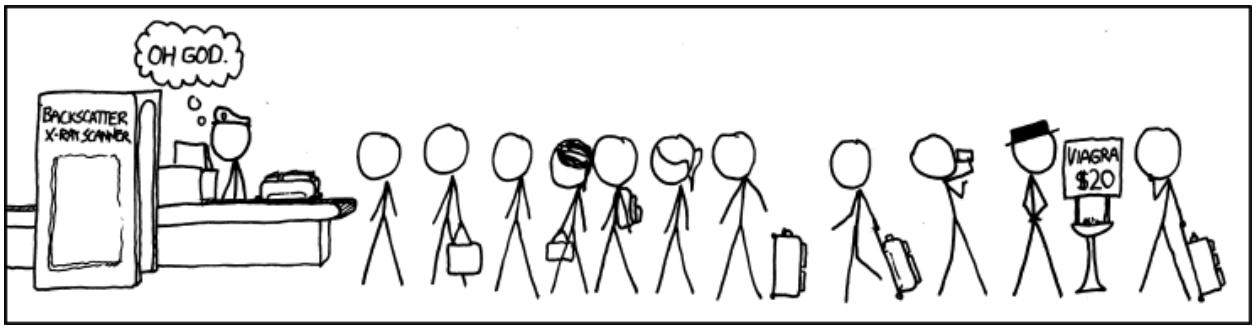
2013 <http://www.tsa.gov/about-tsa>

[9] Richarson, Nigel. "Airport security campaign: The high price of safety." 25 Nov. 2013 <http://www.telegraph.co.uk/travel/travelnews/10460093/Airport-security-campaign-The-high-price-of-safety.html>

[10] Goo, Sara Kehaulani. "Sen. Kennedy flagged by no-fly list." Washington Post 20 (2004): A01.

[11] Gartenstein-Ross, Daveed. "Two cheers for new TSA screening - NY Daily News." 25 Nov. 2013 <http://www.nydailynews.com/opinion/cheers-new-tsa-screening-article-1.1521741>

screening there as well.



Source: "xkcd: Anxiety." 2010. 25 Nov. 2013 <http://xkcd.com/779/>

The National Security Agency is one of the most, arguably the most, intrusive government agency we know of today. In fact, back when the NSA was out of the public eye, it was referred by those in the intelligence community as "No Such Agency". That time is far in the past, and recent accounts on the PRISM program have made it such that it is no longer a question as to whether or not the NSA spies on us, but to what extent. We live in a new age where everyone is a potential enemy to America, even American citizens. This whole article could be written, and many have already been written, about the contributions and subsequent persecutions of NSA whistleblowers such as Bradley Manning and Edward Snowden. However, such an in depth analysis would only prove that which we are already aware, that United States government has increased surveillance on its citizens to the extent that the public expresses outrage upon being made aware of them. But, unlike the TSA, whose work has been attacked as simply a front and unnecessary, the NSA has made many contributions since its inception. Whether those contributions have been ultimately good or bad is hard to discern, given the secret nature of the NSA's work. But it is enough to simply trust that the government will act for the benefit of its constituents without any form of oversight? Of course not, but it is understandable that some aspects of its business must remain private for national security reasons. The problem is that, post-9/11, many laws were enacted that gave far too much power to homeland security in general, and the NSA in particular. The only solution is to amend legislation, a process that will be prolonged extensively, firstly becuase it will take time for the American public to recover from the anti-terrorist frenzy that spurned the Patriot Act and the founding of the TSA, secondly because of the way the American legal system works, and lastly because of the characteristics of bureaucracies.[12]

The Private Sector (402)

There has been staunch objection towards the creation of a universally implemented government database. Cited as a violation of a person's right to privacy, this program was never fully implemented. However, a completely voluntary database is already in existence, and viewed and updated by over 727 million users daily.[13] It's called Facebook, and it's only one of the many online databases made popular throughout the internet revolution. People use it to communicate

[12] Bamford, James. *Body of secrets: anatomy of the ultra-secret National Security Agency*. (sec. 14, 589) Anchor, 2007.

[13] Facebook, Inc. "Key Facts - Facebook." 2012. 25 Nov. 2013 <http://newsroom.fb.com/Key-Facts>

with loved ones, display personal photos, and arrange real-world gatherings. Businesses use it to help customers, advertise products, and even make sales. Facebook, and other social media sites, are becoming more like models for human society, hosting their own sub-communities and economies.

It seems to be somewhat counterproductive to prevent a government database, but encourage private enterprise to create databases of their own. Granted, there is the argument that because these are profit-driven businesses, they would be less inclined to make available your incriminating data for free to those you would rather keep hidden from. However, that also means the contrary is true, that they would be more inclined to sell information to advertisers and interested parties, such as your employers or suspicious relationship partners, probably the people you were trying to keep in the dark anyway. So it is not enough to say that private is better than public, as private corporations have their own goals contrary to your own in regards to your private information.

And the idea of private data itself is somewhat as a misnomer, as if you are tried in court, government agencies can request warrants to access your so called “private” data. And the NSA can even request data without a warrant within the FISA court system, with you never being the wiser. Private companies are required by law to comply with these requests, and aren't even allowed to release the exact number of requests they receive, resulting in the very vague ranges as given in Google's Transparency Report shown below. The end result is that although no universal government database exists currently, an equally intrusive private database is ready whenever the government requires it, and even worse, these private databases are not held under the same restrictions that a public one would be required to adhere to.

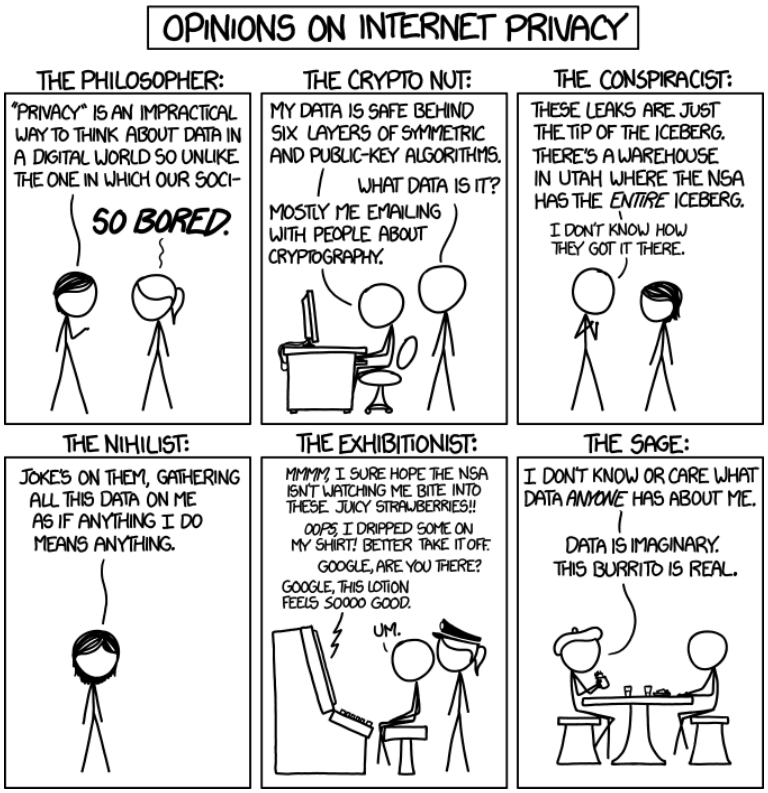
National Security Letters

The table below provides a range of how many National Security Letters (NSLs) we've received and a range of how many users/accounts were specified each year since 2009. For more information about NSLs, please refer to our FAQ. These ranges are not included in the total sum of user data requests that we report biannually.

Year	National Security Letters	Users/Accounts
2012	0–999	1000–1999
2011	0–999	1000–1999
2010	0–999	2000–2999
2009	0–999	1000–1999

Source: "United States – Google Transparency Report." 2012. 13 Dec. 2013

<https://www.google.com/transparencyreport/userdatarequests/US/>



Source: "xkcd: Privacy Opinions." 2013. 25 Nov. 2013 <http://xkcd.com/1269/>

Information Not Found (404)

Taking a page out of James Stacey Taylor's argument noted earlier in this paper, it is generally true that government surveillance would lead to an increase in information, which could potentially lead to more evidence in the event of a crime taking place.[14] And when the crime happens in digital space, such as internet scams and distribution of illegal materials, using digital media as evidence is inevitable. But there is a fundamental danger when using digital media, explained in the following rule:

> Valera's Law: The simpler the medium, the easier to manipulate, and therefore falsify.

Now, this may seem obvious, but when put into practice, it is counterintuitive. In this case, the digital media is simpler than analog. How is this the case? Although the process of hearing a recording stored on a hard drive is more complex to person as opposed to the original person saying it, the amount of information held in those bits are not nearly as much as the detail in the sound waves vibrating the air originally. The perfect microphone does not exist, so it is inevitable that some information would be lost. Citing the ideas of Alfred Korzybski, which states that a perfect map of something cannot exist,[15] digital media is simply a model for a real object or idea, and could never be as detailed as something actually in existence in the real

[14] Taylor, James Stacey. "In Praise of Big Brother" (see footnote #2)
[15] Korzybski, Alfred. *Science and sanity* (see footnote #5)

universe. The proof of this is that the data itself is comprised of matter within the real universe, in the form of electrons or whatnot, and therefore containing something within a subset of itself would result in a contradiction. As a disclaimer to the law, it should be said that by manipulation, it is referring to completely intentional manipulation. Of course, the simple modification of a large organism is easier than modification at the molecular level, however, this is only due to the large scale of the organism, as well as the fact that you are uncertain of the specific molecular consequences your actions will have. In short, although altering large amounts of matter is simple, it can be complicated to reproduce specifically, and therefore not an example of intentional manipulation.

Applied to the idea of digital media and surveillance, this law postulates that digital media is easier to falsify than physical evidence. With consumer programs such as Photoshop and film industry technology such as CGI, photographic and cinematic evidence can be created and altered for a small fee. Of course, currently there is a way to detect modifications, mainly the date modified and subtle mistakes in processing, that could soon change as the technology gets more and more advanced. The result being, soon, digital media manipulation could get so advanced that they could surpass the human perception, and we could only rely on algorithms to spot the fakes. The problem is that computer algorithms are digital as well. What can protect our protectors? Most digital evidence will most likely never be fully accepted in our court systems. Which may end up becoming a major problem when the majority of our interactions and business is done online.

In addition, rather than take the time to modify the evidence, it is much easier to simply wipe memory and destroy physical disks. Because of the compact nature of digital media, it is much easier to make inaccessible. Combined with the fact that the internet is connected over country borders, and data can be accessed and modified from anywhere in the world, then we start to have a problem. If evidence is hosted abroad, the difficulty in obtaining a stable copy for use in court cases gets difficult, as U.S. government officials would have to comply with the laws of the countries they reside in. This problem stems from the general openness of the internet, and many countries have found solutions in creating closed versions of the internet,[16] although this is simply avoiding the problem, as opposed to taking active measures to solve it.

Now, it would be unfair to discuss the security of the internet based on the assumption that digital media is completely insecure. There is the method of encrypting, and as other factors in computing increase in capacity and efficiency, it is not assumed that our cryptographic methods will not evolve with them. However, besides the obvious physical differences, there are important differences between physical and digital security. For this argument, it would be helpful to think of the internet and digital media as a separate dimension from reality, with basing in our physical reality. In this case, the analog counterpart of an encryption scheme would be a lock. This similarity extends to how they are unlocked, with a "key". In the digital plane, you can pick the lock by brute forcing it, another word for simply trying out possible combinations using a script until you arrive at the correct solution. This may seem awfully inconvenient and time consuming, which it is, but it is a simple matter for a computer, and the

[16] Douglas, Bruce. "BBC News - Brazil debates internet law in wake of NSA scandal." 2013. 25 Nov. 2013 <http://www.bbc.co.uk/news/technology-24899396>

time it takes to brute force a specific key is dependent only on the amount of computing power you have on hand.[17] "'Many messages that would have taken hours or days to read by hand methods, if indeed the process were feasible, can now be 'set' and machine decrypted in a matter of minutes... [in reference to the NSA's RYE system]'"[18]

But the analogy to picking a lock is not entirely sound for several reasons. Well, for one, the human element behind picking the lock is no longer there, meaning that there is no "cap" on how fast a computer can compute. With humans, there is the limit of human potential: no matter how much a professional lock-pick practices, there is a threshold that is not physically possible to surpass, maybe due to the structure of our bodies, or the abilities of our minds. The same cannot be said of the digital plane, where processors can be bought with money and computing power improves exponentially. Secondly, as mentioned earlier, digital media, as a simpler form of storage, can be easily duplicated. This property can be abused, for instance, by the government copying encrypted media and then brute forcing the copy without your knowledge. In that case, there is no easy real world analogy. A close one would be the government somehow copying your lock without you noticing, then picking it, making a spare key, then using that key on your original lock. The difference between the two being that while in order to make copy of your lock physically, they would have to stand next to it and presumably examine it for quite a while in order to make a perfect copy. In the digital plane, that process can happen almost instantaneously, and they don't have to physically be in the same room or even the same in country in order to make the switch. And then they are free to use their supercomputers to crack the code in the comfort of their own facilities, taking as much time as they wish.

Now, while digital has many downsides, it would be almost an attack of the premise to completely renounce it. The increased use of digital media is an inevitability in human society, as it is a progression from our analog methods of communications, as well as more efficient and cheaper once the infrastructure is established. And as a simpler form of media, by definition there would be a greater chance of vulnerabilities, but that is a trade-off to how much more accessible it is. The purpose of this argument is not to persuade against the use of technology, but to warn about the potential downfalls of it, and to provoke discussion towards a middle ground between digital and analog. The convenience of digital media pushes all aspects of business to try to implement it as much as they can. However, making everything digital makes information more accessible, which is a benefit when you want to communicate, but also a negative when you sacrifice your privacy in return for convenience.

Redefining Privacy and Property (415)

One of the most difficult parts about determining the ethics of emerging technologies is finding suitable analogies for new inventions. As seen earlier, the perfect analogy does not exist, as it is inevitable that there would be some differences between the digital object and its physical counterpart. The goal is to find objects that have similarities where it matters, and differences which do not affect the outcome of the argument. This quest for the "near perfect analogy" is

[17] Curtin, Matt. *Brute force: cracking the data encryption standard*. (sec. 1, 52-53) Springer, 2005.
[18] Bamford, James. *Body of secrets: anatomy of the ultra-secret National Security Agency*. (sec. 14, 589) Anchor, 2007.

made more difficult by recent intentional efforts by technological companies to refrain from using real world analogies in graphic design.[19] Sometimes, we have to settle for an imperfect analogy, and base our laws around that, which can lead to vague rulings and contradictions. An example of this would be the analogy of hacking private Wi-Fi, called "wardriving", to trespassing, made by John Moor:

> Wardriving might be regarded as trespassing. After all, the wardriver is invading apparently someone's computer system that is in a private location. Conceptually, this would seem to be a case of trespass. But the wardriver may understand it differently. The radio waves are in a public street and the wardriver remains on the public street. He is not entering the dwelling where the computer system is located. Indeed, he may be nowhere nearby.[20]

As our lives get more digital, there will be more and more contradictions like this one, a point that Moor makes in his article.

Another interesting consequence of emerging technology, and one that was not extensively mentioned by any of my sources, would be the effect of artificial intelligence on surveillance. Not the most intuitive combination, but one that will definitely have a major impact on law enforcement the likes we have never seen. James Stacey Taylor went close to this concept when he discussed the consequences of constant surveillance. In his model, the cameras were constantly on, but no one was watching. The tapes would only be accessed as evidence in court. By this reasoning, he stated that the surveillance was not a breach of privacy, even if the cameras were in private places, since a human wasn't on the other end to watch it. This argument would fall flat today, as there is still the chance that someone could view the video. However, since he specified in his premise that the data would be completely under lock and key, we cannot hold against him.[21]

This idea gets more interesting when we consider that by current definition, modern artificial "intelligence" are not considered human, and will not be considered human for at the very least, a long long time. Which raises the question "Does being watched by an AI count as a privacy invasion"? Fortunately, we have a model for that already, in the form of red light cameras. These sophisticated devices serve only one purpose, but serve that purpose very well, and are essentially primitive versions of artificial intelligence. Besides the controversy of authorities implementing them solely to raise funds, they assist in enforcing the law and can be seen as a precursor of things to come. Imagine a near future where cameras are equipped with AI intelligence, and can identify basic crimes. Would having these devices on the street, even without storage capabilities beyond RAM to process the live data, be considered a privacy violation? Probably to an extent, but will the positives outweigh the cost? It is hard to tell, as it depends on how humanoid these AI get, as well as how future legislation defines privacy. But it is undeniable that artificial intelligence will play a part in the evolution of surveillance.

---

[19] "Apple's iOS7, Well, It Was Time For Skeuomorphism To Die - Forbes." 2013. 13 Dec. 2013 <http://www.forbes.com/sites/timworstall/2013/09/19/apples-ios7-well-it-was-time-for-skeuomorphism-to-die/>

[20] Moor, James H. "Why we need better ethics for emerging technologies." Ethics and Information Technology 7.3 (2005): 111-119.

[21] Taylor, James Stacey. "In Praise of Big Brother" (see footnote #2)

Emerging Technology (426)

It would be foolhardy to write an article on surveillance without briefly mentioning the idea of sousveillance, or reverse surveillance. It is true that the proliferation of cheap technology has led to the ubiquity of cameras among the general public, allowing protesters and whistleblowers to document government abuse and spread it online. Do not forget, however, that your cameras can be used against you. As the "Internet of Things" gets closer to reality, the government will have more points of entry to monitor you. Already, many digital cameras come with Wi-Fi support and geo-tagging capabilities. There is even a special SD memory card that you can buy to add this functionality to cameras without it.[22] This, in addition to your smartphone, which probably already has GPS and Wi-Fi built-in, as well as cell tower triangulation and maybe even Bluetooth and RFID capabilities, makes it possible to collect rich data more thorough than simply communications. New devices promise to add even more sensors to exploit. Take, for instance, Google's latest pilot program, Google Glass, an eyewear device that includes a screen and camera to record what you view.[23] Seemingly the perfect sousveillance device, it also includes Google+ Auto Backup to automatically upload the videos you take to your private cloud. Except, as mentioned earlier, nothing is completely "private" on the internet. Another example of questionable technology reaching the power stage would be the new iPhone 5s' TouchID feature, allowing you to unlock your phone with your fingerprint.[24] For now, the prints are stored securely on a chip on the device itself, inaccessible by any other apps you may download. As with all things, this may not be the case in the future.

Conclusion

What conclusions can we draw from this examination? You might have gotten the impression that surveillance has increased dramatically, or that the increase of digital media will lead to more of it in the near future. However, that is not inherently bad. Surveillance is simply observation, and as long as that observation is controlled, it can be used for good. It is up to the reader to decide what extent surveillance should be implemented in society. The problems mentioned in this argument are either a fault against the implementation, or a fault with the technology behind the surveillance. These problems are not inevitable: they can be resolved with improvements to current laws, as well an increased focus in technology in ethical debate. The point being that the surveillance state is not an inevitability, and how our society changes as a result of these surveillance technology depends on us as individuals and as a society. This is a time of change, as our lives get more and more dependent on the digital plane. The way we define our analog ideas to fit new technology will define how laws are made in the future, which will ultimately define the surveillance that takes place in our utopia, or dystopia, depending on our choices.

This is only the current state of surveillance. The real work starts now.

---

[22] "WiFi SD Cards: Eye-Fi Memory Cards: Wireless Photo and Video ..." 2006. 13 Dec. 2013 <http://www.eye.fi/>

[23] "What it Does – Google Glass." 2013. 13 Dec. 2013 <http://www.google.com/glass/start/what-it-does/>

[24] "iPhone 5s: About Touch ID security - Support - Apple." 2013. 13 Dec. 2013 <http://support.apple.com/kb/ht5949>