Surveillance as an infringement on personal space

and tracing of digital footprint

vs

as a balance of privacy

and protection



By: Rahul Gulati

CU ID: 10640249

1. **Introduction**

Surveillance is one of the biggest threats to privacy in the modern world. Countries attempt to portray surveillance as a method to safeguard the rights and freedoms of individuals, but to what extent is this balance acceptable? Surveillance technology like drones have a variety of uses in the current digital space, and this will increase in the post-digital space. Surveillance takes several forms, from drones to webcams, and even wristwatches which track a person’s location. Governments need to be aware if they are invading people’s personal space and backtrack, so a balance between legal oriented surveillance and individual privacy is reached (*Stoddart, Fasken 2019*).

* 1. **Surveillance as an infringement of privacy and how it traces people’s digital footprint**

In January 2020, amid the pandemic, South Korea made detailed location histories of infected people publicly available, which made the public at large aware of who had transmitted the virus, and where it had been transmitted (*Singer & Sang-Hun, 2020*). This led to public shaming and blaming these people for spreading COVID-19. Details like what time people had left for work, and if they wore masks in the train were made publicly available, and any form of the infected people’s privacy (even where they visited) was infringed entirely upon (*Singer & Sang-Hun, 2020)*. However, as other countries increased their surveillance, South Korea suddenly announced that since people did not voluntarily want to get tested for the virus because of privacy concerns, they would start making less data publicly available, which is something many other countries in the world could also follow. In Lombardy, Italy, the government is continuously tracking the location of its citizens (*Singer & Sang-Hun, 2020)*. Through this form of surveillance, the government knows where each person is and how much they move around throughout the day, which is a massive violation of people’s privacy. The government is claiming that 40% of citizens of Lombardy are moving around ‘too much’ (*Singer & Sang-Hun, 2020)*.

The United Nations states that in emergencies, like the pandemic, people must be willing to sacrifice their privacy for the greater good, since data can help improve emergency responses and save lives. The dilemma between people’s morality and privacy arises here (*Singer & Sang-Hun, 2020)*. Unfortunately, the rapid spread of COVID-19 means that governments are setting up mass surveillance systems for selfish purposes as well, and their effectiveness is questionable (*Singer & Sang-Hun, 2020)*.



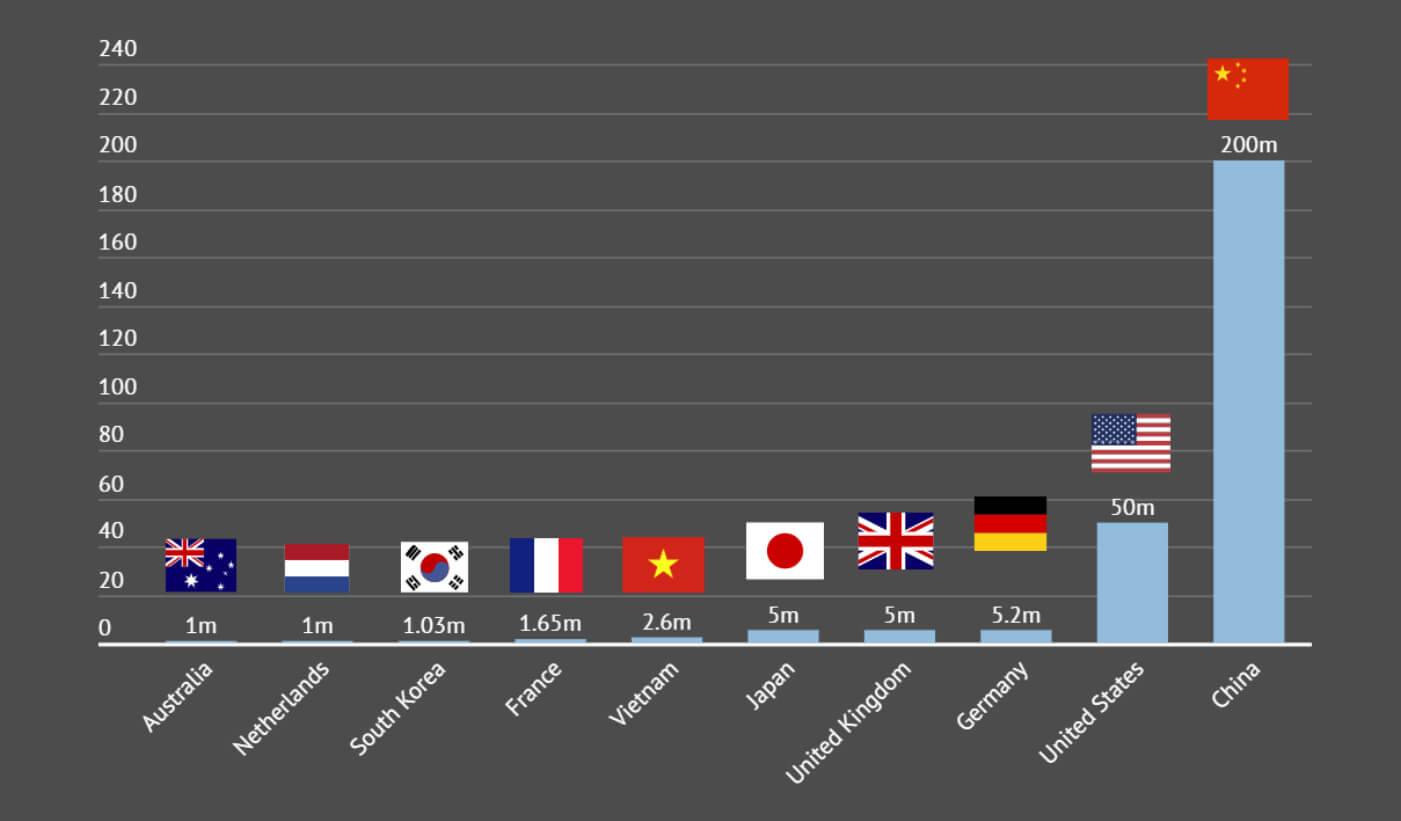
**With an increasing number of surveillance cameras in cities, how much privacy do we have?**

**Source: New York Times**

[**https://www.nytimes.com/2019/02/27/technology/personaltech/digital-footprint-surveillance.html**](https://www.nytimes.com/2019/02/27/technology/personaltech/digital-footprint-surveillance.html)

Another example of an infringement of privacy took place in Mexico. After an Uber passenger got infected with COVID, the government authorities gave Uber the details of the infected person and the details of over 200 other people who had ridden with the same two drivers who had ferried the infected person (*Singer & Sang-Hun, 2020)*. Uber banned the account of both drivers, along with every single person who rode with them. The government and Uber collected the details of these passengers without their permission stating ‘public safety reasons’ (*Singer & Sang-Hun, 2020).*

One of the most extensive undercover surveillance operations in the world was carried out by the United States and the data collected by their National Security Agencies was leaked under the name ‘The Snowden Files’ (*Schuster et al., 2016*). Unscrupulous amounts of data were collected from other countries using the claim that the data was being used for preserving the national security of those respective countries. Data was seized through special software and weak, easily exploitative websites (*Schuster et al., 2016)*. However, the nature of privacy and surveillance that people are affected by is intriguing- people are hesitant to give their fingerprints to governments, but will willingly give them to companies like Apple (*Menand, Louis 2018)*.



**Even though China has the most surveillance cameras in the world, the U.S. tops the list for the greatest number of CCTV cameras per person.**

**Source: TechSpot**

**Link:** [**https://www.techspot.com/news/83061-report-finds-us-has-largest-number-surveillance-cameras.html**](https://www.techspot.com/news/83061-report-finds-us-has-largest-number-surveillance-cameras.html)

In 2002, in New York City, the police arranged the setting up of a ‘centralised surveillance centre’ which would access thousands of CCTV cameras across New York, once again raising the debate between security and privacy of individuals (*American Civil Liberties Union, 2002)*. Results from an independent report found that 80% of ‘criminals’ identified by the London Police’s Facial Recognition Software were innocent, which caused anger among citizens (*Bhatia, Gautam 2019*).

If mass, facial surveillance incorrectly identifies people as criminal offenders, it raises concerns about the other dangers of surveillance, primarily surveillance powered by Artificial Intelligence (*Bhatia, Gautam 2019)*.

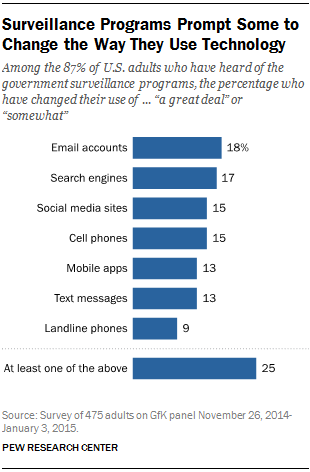


**How effective is facial recognition surveillance when detecting crime?**

**Source: Debating Europe**

[**https://www.debatingeurope.eu/focus/arguments-for-and-against-government-surveillance/**](https://www.debatingeurope.eu/focus/arguments-for-and-against-government-surveillance/)

After this incident, San Francisco, a technologically-savvy city, altogether banned facial surveillance technology (*Bhatia, Gautam 2019)*. However, despite this incident, Indian law-makers demanded the creation of an ‘Automated Facial Recognition System’ projecting it as a method that will help identify criminals using information from CCTV cameras (*Bhatia, Gautam 2019)*. This data would then be stored by the National Crime Records Bureau (NCRB) of India, which once again raises the question of what the government would do with this information (*Bhatia, Gautam 2019)*. How much surveillance footage is recorded, and how much is stored? Do people truly have any privacy in the current digital space?



**A survey of 475 Americans shows how people use technology differently because of surveillance**

**Source: PEW Research Centre**

[**https://www.pewresearch.org/fact-tank/2018/06/04/how-americans-have-viewed-government-surveillance-and-privacy-since-snowden-leaks/**](https://www.pewresearch.org/fact-tank/2018/06/04/how-americans-have-viewed-government-surveillance-and-privacy-since-snowden-leaks/)

In Hong Kong, quarantined people were required to wear a wristband linked to an app which would notify the government if that particular person left the quarantine centre (*Kharpal, Arjun 2020)*. An Israeli security agency, Shin Bet is using location data to track virus cases as well, but concerns have been raised that this company has been collecting people’s data for years, supposedly for counter-terrorism purposes (*Kharpal, Arjun 2020)*.

Phones of journalists all over the world, from Bahrain to Morocco are hacked by security companies to see what they are saying (*Nyst, Carly 2018*). The government’s invasion of privacy in a person’s private life or workplace prevents the individual from exercising their right to freedom and expression, which is a basic fundamental right (*Nyst, Carly 2018).* To analyse the extent that surveillance affects us, we need to think about our past. People could communicate with others, join groups anonymously and travel to different countries without anyone knowing, but now the government tracks our every movement (*Nyst, Carly 2018)*.

By reducing their digital footprint, people can effectively reduce the amount of surveillance done on them to some extent (*Mozur, Paul 2019)*. In a New York Times Investigative Journalism Piece titled ‘Limiting your Digital Footprints in a Surveillance State’, journalist Paul Mozur says that China has over 200 million surveillance cameras, which is more than anywhere else in the world (*Mozur, Paul 2019*). He says that the government controls all the phone companies, and data must be handed over when demanded, and so phone numbers can be liabilities. Two-step authentication processes for certain apps can help reduce the chance of accessing sensitive data. The messaging app WeChat is also under constant surveillance by the government (*Mozur, Paul 2019)*.



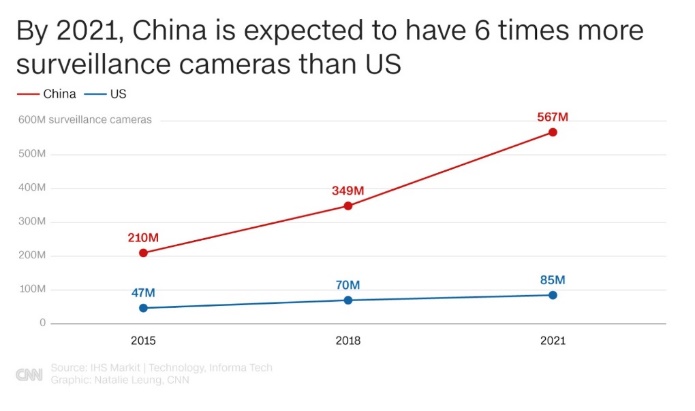
**Paul Mozur explains that carrying two phones with identical cases can help reduce a person’s digital footprint to some extent.**

**Source: New York Times**

**Link:** <https://www.nytimes.com/2019/02/27/technology/personaltech/digital-footprint-surveillance.html>

In China, police demand to see a person’s phone to delete photographs, which is a massive infringement of privacy, but it is present in a communist state, and no equilibrium can be reached in this case (*Mozur, Paul 2019).* Paul says that, in such a situation, carrying two phones with the same case is beneficial, so that a person’s digital footprint cannot be traced as effectively. Contact tracing apps trace people’s digital footprint, including the places that they visit and how long they are there for (*Guinchard, Audrey 2020)*.

In rare cases, due to the coronavirus, China has installed security cameras inside people’s homes enabling the government to monitor people very closely (*Gan, Nectar 2020)*. If the post-digital space involves continuous government surveillance inside our own homes, the concept of privacy may become non-existent (*Gan, Nectar 2020)*.



**By 2021, China is expected to have 567 million surveillance cameras**

**Source: CNN.**

**Link:** [**https://edition.cnn.com/2020/04/27/asia/cctv-cameras-china-hnk-intl/index.html**](https://edition.cnn.com/2020/04/27/asia/cctv-cameras-china-hnk-intl/index.html)

* 1. **Surveillance as a form of protection while maintaining privacy**

Lawrence Cappello, a professor at the University of Alabama, gives the example of America and emphasises the fact that the country’s formation partly took place due to rebellions against the British, who had violated Americans’ privacy (*K.N.C., 2019*). Hence, he says that the issue of privacy is an ancient concept, but the technological advancements made in the surveillance field are incredibly alarming (*K.N.C, 2019)*.

In 2018, a survey revealed that 22% of companies around the world are monitoring employees, including their computer and calendar-usage data, which is a massive threat to privacy (*Sheng, Ellen 2019*). The monitoring of social media accounts of employees aims to prevent the tarnishing of the company’s reputation. Companies claim that this information is collected to increase productivity, but the truth may be very different (*Sheng, Ellen 2019*).

In both the current and post-digital space, surveillance in the workplace must follow the laws of the country to ensure violation of an employee’s privacy does not occur, and it is the company’s responsibility to ensure that employees have a harassment-free workplace (*Sheng, Ellen 2019)*.

However, the opposing argument states that surveillance is essential for the safety and protection of the people (*K.N.C*, *2019*). For example, the police need to use surveillance in public spaces to monitor crime, and employers need to observe employees in the workplace to ensure that they are performing their tasks effectively (*K.N.C 2019)*. In 2014, in the United States, Timothy Carpenter was convicted of conducting several armed robberies, and phone tower data was used to continuously monitor him, which ultimately led to his arrest (*Menand, Louis 2018*). Is this a breach of fundamental human rights or do his criminal activities warrant being tracked? Can tracking him be a reasonable ‘excuse’ to use surveillance in this particular case? It is impossible to achieve a situation where every person will abide by the rules, and so, surveillance is essential.



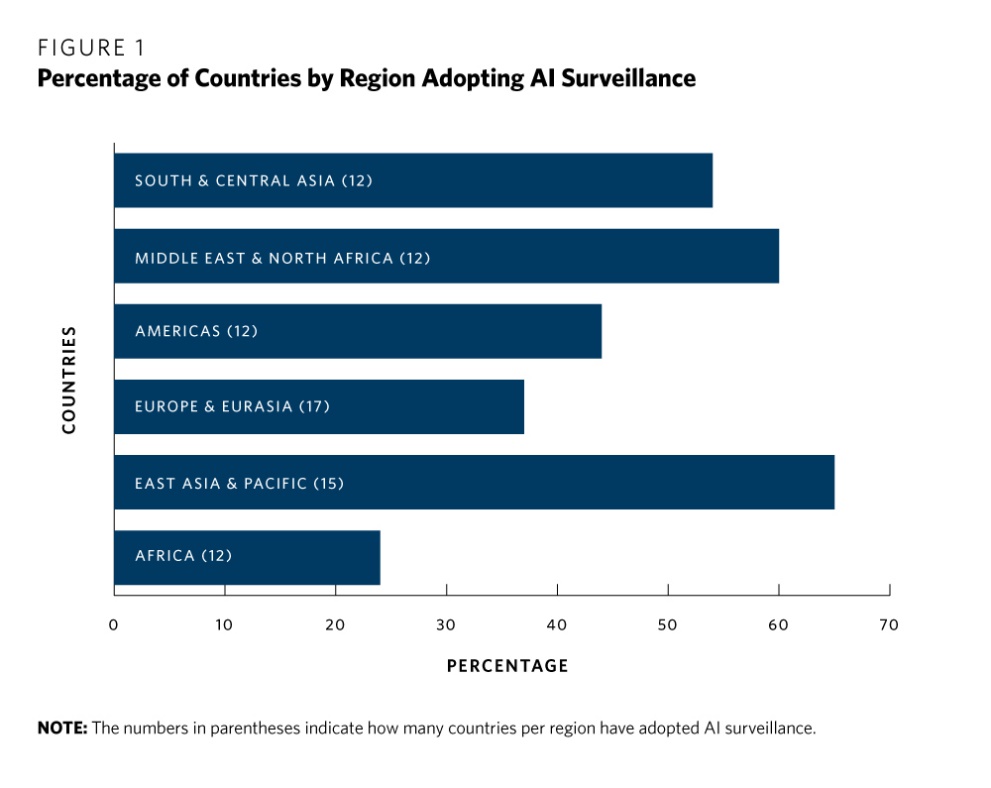
**Surveillance cameras are used by law-enforcement agencies all over the world in hopes to reduce crime.**

**Source: Source Security**

**Link:** [**https://www.sourcesecurity.com/news/belgian-police-full-hd-sony-4-surveillance-cameras-secure-crime-co-289-ga-co-2566-ga-co-11239-ga-co-1515580835-ga.1548056311.html**](https://www.sourcesecurity.com/news/belgian-police-full-hd-sony-4-surveillance-cameras-secure-crime-co-289-ga-co-2566-ga-co-11239-ga-co-1515580835-ga.1548056311.html)

Due to the current coronavirus situation, several cities in China have placed surveillance cameras outside quarantined people’s homes to ensure they do not leave their houses (*Gan, Nectar 2020*). People are enraged since this is a massive violation of their privacy, but they have no choice but to accept this (*Gan, Nectar 2020)*. However, these measures have been taken to ensure that people in quarantine abide by the strict rules in place. This reduces the risk of spreading the virus, thereby protecting a large section of society.

Rapidly progressing technology has enabled law enforcement agencies in the United States to have an opportunity to increase their surveillance activities (*Holmes, Aaron 2020*). Surveillance is used to monitor protests to ensure that they do not go out of control, thereby reducing chances of riots which only have catastrophic consequences. Reaching a balance between the amount of surveillance conducted and the freedoms of individuals is essential. (*Holmes, Aaron 2020*).

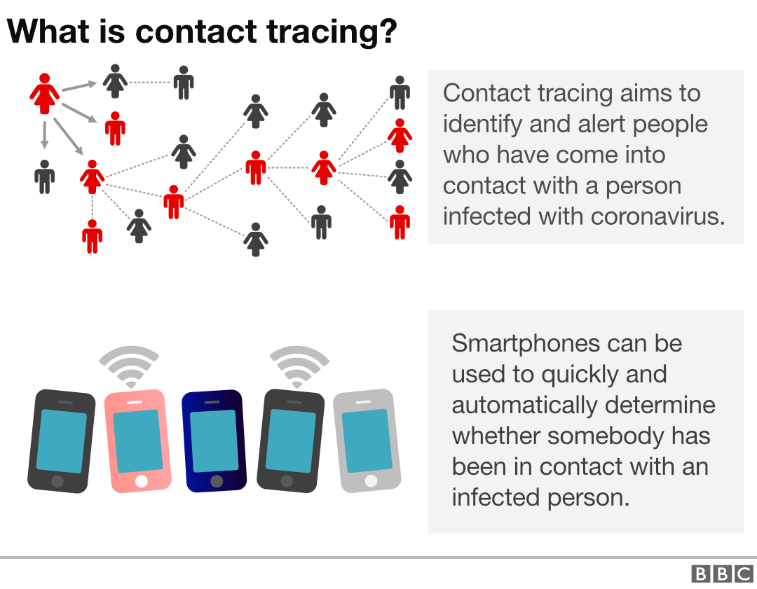


**The number of countries that have adopted surveillance techniques**

**Source: Carnegie Endowment for International Peace**

**Link**: <https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847>

Countries like Israel, South Korea and Singapore are making use of location-based tracking, surveillance cameras and credit card information during the time of COVID-19 (*Kharpal, Arjun 2020)*. These countries claim that this information is used to keep track of where their virus cases are arising from so that they can deal with them effectively.

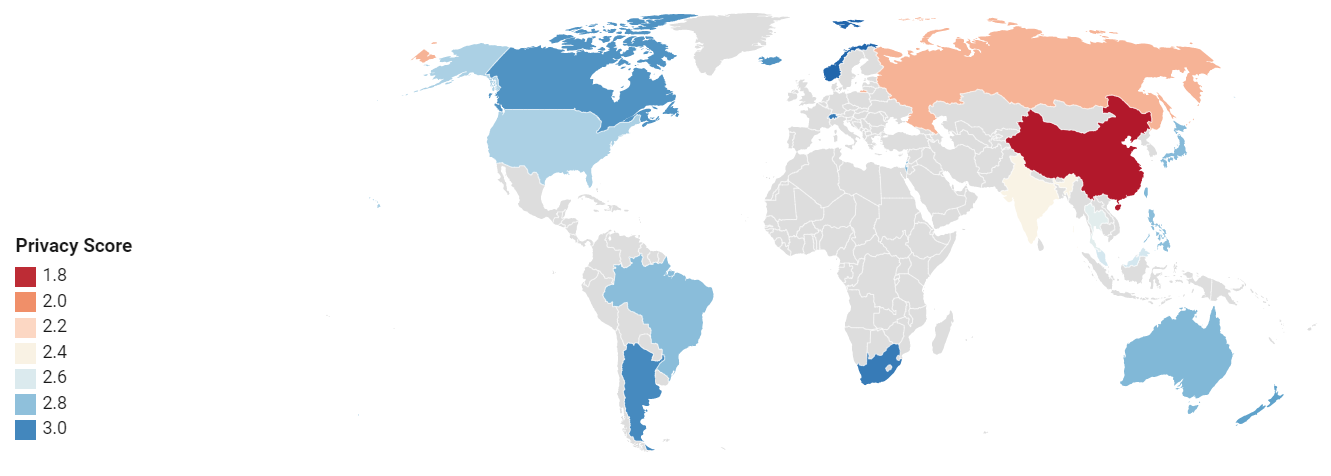


**Contact Tracing is used by countries to detect virus cases to keep people safe**

**Source: BBC**

**Link:** <https://www.bbc.com/news/technology-52353720>

Comparitech assessed surveillance and privacy in 47 countries, and the results are alarming. The usage of fingerprint and facial recognition technology is increasing worldwide. Only five countries in Europe provide adequate privacy protection for their citizens (*Bischoff, Paul 2019)*. Concerns arise that the protection offered by these countries is only ‘adequate’, but the privacy offered by the other assessed countries is far more concerning. The countries which scored the highest were Ireland, France, Portugal, Denmark and Malta (*Bischoff, Paul 2019)*. The worldwide assessment showed that China, Russia, India, Thailand and Malaysia were at the bottom of the list, offering limited safeguards and weakened protections, while China’s extensive surveillance with little or no safeguards was incredibly alarming (*Bischoff, Paul 2019)*. Italy does not have freedom of the press, so only government propaganda is conveyed by the media. The usage of facial recognition in airports and excessive CCTV monitoring causes concern among citizens (*Bischoff, Paul 2019).*



**Privacy scores in different countries show the extent of surveillance in each country, and how some countries are adopting better privacy protection laws than others.**

**Source: CompariTech**

[**https://www.comparitech.com/blog/vpn-privacy/surveillance-states/**](https://www.comparitech.com/blog/vpn-privacy/surveillance-states/)

Hence, the demand for a balance between people’s privacy and their rights must be reached, and several countries around the world have begun adopting policies to reach an equilibrium (*National Law Review, 2020)*. The General Data Protection Law in Brazil (LGPD) requires the consent of a guardian (if a child is under 12 years old) to process the data of the child, and individuals also have the right to be informed of how their data will be used (*National Law Review, 2020)*. This law is incredibly powerful because it gives Brazilians the right to access and delete their personal data, as well as keep a portable copy of the same.

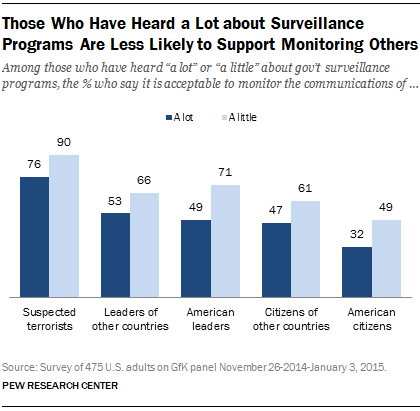
However, the law allows collection of data for law enforcement (public safety) and national defence purposes, raising questions about what the data collected here is used for (*Stauss, David 2020)*. The law exempts people’s consent for the use of their data when it comes to ‘legal purposes’ which increases the scope for government loopholes which would effectively threaten citizens’ privacy (*Stauss, David 2020*).

In April, in the United States, the government started talks with tech companies like Google and Twitter about using location data captured for virus-spreading surveillance purposes, and the Congress highlighted the importance of safeguarding people’s privacy during these talks (*Singer & Sang-Hun, 2020)*.

Data protection laws in general focus on ‘personal data’ and helping people deal with violations of the same, but the regulations in place are not effectively monitored, resulting in data breaches where people are helpless (*Schuster et al., 2016)*. Baseline security regulations should be set up in countries to ensure that the extent of surveillance is less massive than the current scenario.

Striking a balance between how much surveillance is carried out, and the amount of privacy people have without being monitored continuously is paramount (*Schuster et al., 2016)*. The Snowden incident should have ensured that countries decrease their mass surveillance activities; however, the opposite seems to have taken place.

In the United States and European Union, governments have held discussions about improving privacy and making amendments to their surveillance activities, but very few changes have actually taken place (*Schuster et al., 2016)*. Countries need to recognise that public space surveillance must also ensure that a reasonable level of privacy is also maintained (*Stoddart, Fasken 2019*).



**Comparison of support of surveillance among two groups of people**

**Source: PEW Research Centre**

[**https://www.pewresearch.org/internet/2015/03/16/americans-views-on-government-surveillance-programs/**](https://www.pewresearch.org/internet/2015/03/16/americans-views-on-government-surveillance-programs/)

**Conclusion**

‘Protection from terrorist attacks’ is the primary justification given to increase surveillance around the world. However, terrorists are not deterred by CCTV cameras (*American Civil Liberties Union, 2002)*. These cameras have the opposite effect- they may attract more suicide bombers since it helps them gain media coverage for their terrible acts. The actual reason why surveillance cameras have been set up is to reduce the frequency of ‘small crimes’, but as seen in Britain, there has been no reduction in crime even after deploying these cameras (*American Civil Liberties Union, 2002*). If surveillance cameras are not serving their real purpose, why are they still needed?

If people know they are being watched, they would be more conscious about their speech, their interactions or even what materials they read or what content they watch, which makes the dangers of crime increase and any benefits of surveillance will be lost. Freedom of the media is pointless if there is constant surveillance on the matter being published. Hence, in conclusion, a dexterous balance between privacy and surveillance for protection must be achieved, in which surveillance only plays a role in preventing crime without infringing on an individual’s privacy.

The greatest danger of surveillance is that it can be misused by law enforcement agencies and governments (*American Civil Liberties Union, 2002*). During the Vietnam war, for example, law enforcement agencies across the U.S. illegally used surveillance to harass challengers of racial segregation. Biases are dangerous to surveillance activities as well- In Britain, law enforcement agencies were accused of targeting mostly people of colour for surveillance, instead of tracking the people who needed to be tracked (*American Civil Liberties Union, 2002*). Corrupt police officers and government officers can misuse surveillance to target and harass innocent people in exchange for money, or because they are in a position of power (*American Civil Liberties Union, 2002*).

**References**

1. K.N.C (2019). The Economist. *Surveillance is a fact of life, so make privacy a human right*. [online] Available at: <https://www.economist.com/open-future/2019/12/13/surveillance-is-a-fact-of-life-so-make-privacy-a-human-right>. [Accessed 12 Oct. 2020].
2. Bhatia, G. (2019). Hindustan Times. *Facial surveillance is a threat to privacy*. [online] Available at: <https://www.hindustantimes.com/columns/facial-surveillance-is-a-threat-to-privacy/story-hjtQCSMbpGteftjuzzB7cN.html> [Accessed 13 Oct. 2020].
3. Sheng, E. (2019). Employee privacy in the US is at stake as corporate surveillance technology monitors workers’ every move. *CNBC* [online]. Available at: <https://www.cnbc.com/2019/04/15/employee-privacy-is-at-stake-as-surveillance-tech-monitors-workers.html> [Accessed 10 Oct. 2020].
4. Stauss, D. (2020). Security Magazine. *What U.S. companies should know about LGPD – Brazil’s new General Data Protection Law*. [online] Available at: <https://www.securitymagazine.com/articles/93430-what-us-companies-should-know-about-lgpd-brazils-new-general-data-protection-law> [Accessed 13 Oct. 2020].
5. National Law Review (2020). *Brazilian Government Makes the LGPD Effective Imminently*. [online] Available at: <https://www.natlawreview.com/article/brazilian-government-makes-lgpd-effective-imminently> [Accessed 13 Oct. 2020].
6. Holmes, A. (2020). *How people are using technology like drones, and facial recognition to monitor protests and track people across the US.* [online] Business Insider. Available at: <https://www.businessinsider.com/how-police-use-tech-facial-recognition-ai-drones-2019-10> [Accessed 13 Oct. 2020].
7. Bischoff, P. (2019). Comparitech.com. *Surveillance States: Which countries best protect privacy of their citizens? - Comparitech*. [online] Available at: <https://www.comparitech.com/blog/vpn-privacy/surveillance-states/>. [Accessed 11 Oct. 2020].
8. Kharpal, A. (2020). *Use of surveillance to fight coronavirus raises concerns about government power after pandemic ends*. [online] CNBC. Available at: <https://www.cnbc.com/2020/03/27/coronavirus-surveillance-used-by-governments-to-fight-pandemic-privacy-concerns.html>. [Accessed 9 Oct. 2020].
9. Gan, N. (2020). China is installing surveillance cameras outside people’s front doors… and sometimes inside their homes. *CNN,* [online]. Available at: <https://edition.cnn.com/2020/04/27/asia/cctv-cameras-china-hnk-intl/index.html> [Accessed 8 Oct. 2020].
10. Schuster, S., Van Den Berg, M., Larrucea, X., Slewe, T. and Ide-Kostic, P. (2016). Mass surveillance and technological policy options: Improving security of private communications. *Computer Standards and Interfaces*, [online] 50, pp.76–82. Available at: <https://www.sciencedirect.com/science/article/pii/S0920548916300988> [Accessed 11 Oct. 2020].
11. Singer, N. and Sang-Hun, C. (2020). As Coronavirus Surveillance Escalates, Personal Privacy Plummets. *The New York Times*. [online]. Available at: <https://www.nytimes.com/2020/03/23/technology/coronavirus-surveillance-tracking-privacy.html>. [Accessed 10 Oct. 2020].
12. Menand, L. (2018). *Why Do We Care So Much About Privacy?* [online] The New Yorker. Available at: <https://www.newyorker.com/magazine/2018/06/18/why-do-we-care-so-much-about-privacy>. [Accessed 12 Oct. 2020].
13. Stoddart, F.-J. (2019). *Having Privacy in Public: Limits to Unwanted Surveillance in Public Spaces | Lexology*. [online] www.lexology.com. Available at: <https://www.lexology.com/library/detail.aspx?g=d04b0a48-5d03-42a7-9a04-9808de659a4d>. [Accessed 9 Oct. 2020].
14. American Civil Liberties Union (2002). *What’s Wrong With Public Video Surveillance?* [online] Available at: <https://www.aclu.org/other/whats-wrong-public-video-surveillance>. [Accessed 11 Oct. 2020].
15. Nyst, C. (2018). *Two sides of the same coin – the right to privacy and freedom of expression*. [online] Privacy International. Available at: <https://privacyinternational.org/blog/1111/two-sides-same-coin-right-privacy-and-freedom-expression> [Accessed 13 Oct. 2020].
16. Mozur, P. (2019). Limiting Your Digital Footprints in a Surveillance State (Published 2019). *The New York Times*. [online] 27 Feb. Available at: <https://www.nytimes.com/2019/02/27/technology/personaltech/digital-footprint-surveillance.html>. [Accessed 12 Oct. 2020].
17. Guinchard, A. (2020). Our digital footprint under Covid-19: should we fear the UK digital contact tracing app? *International Review of Law Computers & Technology*. [online] Available at: <https://www.researchgate.net/publication/342960099_Our_digital_footprint_under_Covid-19_should_we_fear_the_UK_digital_contact_tracing_app> [Accessed 13 Oct. 2020].

**Picture References**

1. Aamir, Huzama (2019). TechSpot. *Report finds the US has the largest number of surveillance cameras per person in the world*. [online] TechSpot. Available at: <https://www.techspot.com/news/83061-report-finds-us-has-largest-number-surveillance-cameras.html> [Accessed 13 Oct. 2020].
2. Debating Europe. (n.d.). *Arguments for and against government surveillance*. [online] Available at: <https://www.debatingeurope.eu/focus/arguments-for-and-against-government-surveillance/#.X4Vbb9AzY2w> [Accessed 13 Oct. 2020].
3. Geiger, A. (2018). *How Americans have viewed government surveillance and privacy since Snowden leaks*. [online] PEW Research Centre. Available at: <https://www.pewresearch.org/fact-tank/2018/06/04/how-americans-have-viewed-government-surveillance-and-privacy-since-snowden-leaks/>. [Accessed 11 Oct. 2020].
4. Source Security (n.d.). *Belgian police install high-end Full HD Sony 4K surveillance cameras to secure streets and fight crime in Lokeren*. [online] Available at: <https://www.sourcesecurity.com/news/belgian-police-full-hd-sony-4-surveillance-cameras-secure-crime-co-289-ga-co-2566-ga-co-11239-ga-co-1515580835-ga.1548056311.html> [Accessed 13 Oct. 2020].
5. Feldstein, S. (2019). *The Global Expansion of AI Surveillance*. [online] Carnegie Endowment for International Peace. Available at: <https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847>. [Accessed 11 Oct. 2020].
6. Kelion, L. (2020). Why are there doubts over contact-tracing apps? *BBC News*. [online] 20 Apr. Available at: <https://www.bbc.com/news/technology-52353720>. [Accessed 12 Oct. 2020].