Issue of surveillance to track cybercrime

🌎DO YOU AGREE TO THE TERMS AND CONDITIONS OF SURVEILLANCE?

– A discussion on the fine print of relational surveillance –

The following essay will address the matter of surveillance as a method used to track and deter cybercrime. This will be accomplished by consulting theories as maintained by David Lyon in defining surveillance according to his examinations and critiques thereof. Following this, additional connections will be made between observations surrounding surveillance theory provided by other individuals in the field. Moreover, the paper will briefly illustrate the ideas of the Panopticon as proposed by Jeremy Bentham and their relevance to the concept of surveillance in contemporary society. By extension, this section will include references to Foucault. Subsequently, notions of ambiguity, resistance and exposure will be integrated into the overall discussion as a means of illuminating the ironic and paradoxical situation of breaching privacy as a means of avoiding the breach of privacy. In closure, the essay will conclude with a view that explains why data collection, even though sometimes helpful, remains invasive at the expense of individual privacy.

David Lyon writes extensively on the subject of surveillance and defines it as “ the focused, systematic and routine attention to personal details for purposes of influence, management, protection or direction” (2007: 14), which he explains as being derived from the French meaning to ‘ watch over’. The central themes in Lyon’s literature are those which focus on critical examinations of the nature of surveillance, its purpose and its impact (and potential impact) on daily life. In his 2001 work titled *Surveillance*

Society: Monitoring Everyday Life, Lyon maintains that individuals are responsible for their own loss of privacy and are complicit in it.

Lippert (2008) draws on Lyon's work, maintaining that " surveillance is intrinsically ambiguous" (2008: 470). Furthermore, he illuminates the variances between using surveillance to enhance safety versus using surveillance to exert control. Lippert uses contrasting examples of a lifeguard at the beach and a police officer on a stakeout in order to illustrate these variances. Lippert's discussion extends to ' heuristic devices' (2008: 472) of observation, which he believes to be present in any given surveillance system. This view is shared with Lyon, who outlines three types of relational surveillance: face-to-face, file-based and electronic. Lippert, agreeing with Lyon, concludes that surveillance is ' ambiguous and not without resistance' (2008: 472-473).

Saulnier (2017) provides an account of the role of resistance in surveillance. She comments on a mixture of literature, essentially observing that surveillance denotes power and power denotes resistance. This observation is made according to her revisions on what is referred to as the " surveillance capital", a term used to describe the presence, use and resistance to surveillance (2017: 287). Saulnier is not the first to comment on the resistance to surveillance in the context of crime, as this has been done by authors such as McCahill and Finn (2014: 4), who discuss the confrontation between the surveilled an the surveilled in a study using a variety of social groups such as police officers and offenders. The concept of resistance is significant in discussions of surveillance as it would not exist if it

was not for and debates about privacy and liberty, and the infringements or violations thereof.

Ball (2009), places external exposure and internal self-vulnerability as a means of theoretically explaining how individuals will react to being surveilled. She explains that responses to encountering surveillance range from acceptance to resistance. Surveillance should be required and not automatic. Essentially, the resistance to surveillance is due to the lack of transparency (actual or perceived) that is experienced by an individual. Many forms of surveillance expose individuals to harmful cybercrimes, and they become subject to agreeing to potentially violate their privacy which is unnecessary and ineffective in the bigger picture of fighting cybercrime. Using surveillance to monitor crime in a cyber environment should be more focused on criminal behavior characteristics and trends, rather than on personal data collection that is beneficial for governmental and corporate spheres. In saying this, *Mrs. XYZ* providing her gender or other private details will not be entirely necessary to decrease cybercrime.

Therefore, tailoring surveillance enhances the trust and transparency of the relationship between agencies and internet users. Surveillance should thus be applied in a manner that is reasonable and proportionate. This is akin to the ‘ use of force’ method followed by law enforcement in England and Wales. For example, using online grocery shopping to demonstrate, saving card details or addresses on online purchasing sites is proportionate. However, surveillance focused on information such as gender do not share the same proportionality when doing online shopping. To put it bluntly, stating whether one is male or female will not contribute to the monitoring or

deterrence of cybercrime. When using surveillance, it is important to remain transparent and be explicit. This would be ideal and beneficial because the process then becomes both informative and deterrent, creating the possibility and probability of both.

According to Sloan and Warner (2017: 2), surveillance that occurs contemporarily is “ constant, pervasive and invasive”. The authors are describing the surveillance that takes place when collecting the personal information and details of patients within the public health environment. They debate that this information collected has “ provided the foundation for [the] planning, intervention and prevention of disease” (2017: 4), however, they also provide comment on the appropriateness of the extent to which this information is collected. This notion of how much surveillance is appropriate or reasonable is a common theme in debates surrounding the infringement of personal privacy. The unreasonable range of data collected about individuals is justified by the ‘ safety’ it *could* provide in the name of cybersecurity, at the expense of the individuals liberty.

Ball(2009: 607) posits that there are several elements of exposure. Those that are threatening to privacy shall be consulted. Ball suggests that the nature of what is exposed is dependent on the level of intrusiveness of the surveillance. She believes that this is “ made problematic by remote and silent data collection” (2009: 607). Secondly, Ball suggests that exposure depends on the individual’s prior knowledge of the surveillance methods and by extension, their implications. Ball poses important comments regarding the relationship between surveillance and exposure. Amongst various definitions of exposure provided by this author, the “ state of being

vulnerable or exposed” (2009: 608) holds relevancy. In saying this, the surveillance encapsulating daily ‘ cyberuse’ by individuals creates just as much of a threat to privacy and liberty than that of becoming a victim of cybercrime. Collecting personal data as a means of resolving cybercrime is still leaving the individual vulnerable and exposed.

Notions of surveillance as counterproductive or causative are not new in ‘ cyberstudy’. Strandburg (2008) says that the “ characteristics of modern communications that enhance association also enhance the potential that association will be chilled by relational surveillance” (2008: 5). The result is that of a *catch 22* , using personal data to protect personal data, giving up privacy to protect privacy.

Similarly, Nelken (2014) maintains that as individuals of the state, “ we govern through crime [and the promise of security] but also crime is produced through our governing” (2014: 405). Nelken elaborates by stating that the results yielded by acting against cybercrime are twofold. On the one hand, there are “ good reasons to act against the misuse of cyberspace” (2014: 410). For example, through the “ use of indicators to measure what is happening” as a way to collect data that may “ improve health” and wellbeing (2014: 410). On the other hand, the use of indicators “ can be just as much the problem as the solution” (2014: 410).

Matthews and Kauzlarich (2007) provide a discussion on the success of the state in using surveillance to identify several instances of crime. However, they maintain that the state is “ not quick to define their own actions as criminal” (2007: 47). This issue is one that is theoretically hypocritical. In

saying this, individuals have a right to privacy and safety that should not be violated. This is something preached and promised by the government, however, it should not be overlooked that the government tends to violate their own laws, ultimately failing to practice what they preach. In cases where the government will wiretap personal devices and follow individuals, an infringement and violation of the right to privacy is undeniable, however this is justified in the name of upholding the law.

In his article, Thomas McMullan reports that Jeremy Bentham's skeleton is on display at the University College London. As per his request, Bentham was dissected and placed in a glass case on public display. According to McMullan, his cadaver contains " a webcam that records the movements of its spectators and broadcasts them live" (2015, [online]). The purpose of this is for the University's " Panopticam Project", which hopes to inspire students to engage in debates about the state of contemporary surveillance. The project is named after Bentham's proposal of the Panopticon, a building designed to monitor prisoners.

Much literature surrounding cybercrime and the monitoring thereof tends to draw inferences between the panopticon and the surveillance of cyberthreats (or crime). Even though there are certain similarities in theory, these are not physical and should be explicitly understood as a metaphor rather than a comparison. The inmates jailed in the Panopticon experience constant awareness of being watched from a tower, encouraging them to engage in suitable behaviour. The idea is powerful in that it remains influential in the absence of a physical presence. In other words, inmates are

unaware of when they are being monitored and thus should act accordingly at all times.

The surveillance of individuals' private information over the internet is similar in its theoretical approach but not in its physical. This means that in theory, individuals are aware of being watched but still feel as though their browsing and cyber activity is somewhat private since there is no physical authoritative presence such as the tower faced by prisoners in the Panopticon. Furthermore, the sense of privacy experienced by individuals in the ' cybersphere' may increase their sense of anonymity, a contrasting effect to being exposure to physical methods of authority. McMullan comments on this fact, saying that the " internet is not a prison. We're generally there voluntarily. Unlike the prisoners we can avoid being seen by staying off the net" (2015, [online]).

As mentioned, the notion of an electronic panopticon is a common theme in writings on surveillance. Foucault revived the concept of the Panopticon as proposed by Bentham in his work titled – Discipline and Punish: The Birth of the Prison. Written in 1975, Foucault draws on the ideas of Bentham to make comments on punishment within the social context. To summarise, Foucault proposes that the need for surveillance is what resulted in the proposal of a panopticon. He claims that a fully efficient institution is one that exerts persistent and omnipresent monitoring that induces the sense of permanence and ensures that power is optimal.

Miller (1995: 2) reports that the FBI employ a program known as Carnivore, which monitors all incoming and outgoing email. Miller explains that this type

of program is “ a variation of software…typically used by Internet Service Providers (ISP’s) known as a packet sniffer”. This program is not the only of its kind, it shares characteristics with other software’s designed to search for ‘ keywords’ within emails. Furthermore, the panopticon model may be implemented on the basis that it is “ perceived by users as a necessity… convinced that such a structure would protect them” (Miller, 1995: 14).

There is irony in the availability of cybersecurity programs that determine the extent of data usage or perceptibility to surveillance by doing the very same thing. It seems that the modern surveillance culture in contemporary society is constant in its presence, even when changing in its methods. Surveillance experienced on a daily basis is not designed to be malicious. For example, marketing tools may employ surveillance as a means of becoming more familiar with clientele. However, even if this is intended to benefit consumers in some way, it is still invasive in its method. Sheridan (2016) believes that contemporary culture has “ entered into a social contract where those perceived breaches of privacy are considered to be the price we pay to be safe and ensure our continued security” and further comments on how it is “ easy to forget that we are under observation, because the watchtower has been deconstructed” (2016: 6).

Even thoughdata collection has proven to be positive in its provision of expediency, it remains invasive. Noted by Sheridan who maintains that “ the [surveillance] system spreads intrusively under the guise of convenience” (2016: 49). He explains that the collection of this data has been successful in identifying crimes such as identity theft through its flagging of suspicious

spending patterns however, the fact still remains that the “ data is stored somewhere, and someone has complete access to it” (2016: 74).

Dupont (2008) takes a unique stance in his writing on the panopticon and surveillance. He produces one of the few pieces of literature available that is active in its approach, making suggestions rather than just reporting on privacy infringements. He discusses the tool of cryptography and how it is available to those who feel that their liberties are being disturbed.

Cryptography is defined as being associated with the process of converting ordinary plain text into unintelligible text and vice-versa. It is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. Cryptography not only protects data from theft or alteration but can also be used for user authentication (Economic Times, 2019 [online]).

This safeguard is widely available but not widely known. He notes that “ most popular email programs such as outlook can send and receive encrypted emails, but very few people actually use this facility” (2008: 272). Correspondingly, Garfinkel and his colleagues conducted a study in 2005 in order to determine whether people took these cryptographic precautions as a means of protecting their data. The results showed that 68% of people were not aware that the option of encrypting emails was available to them. Additionally, Dupont (2008: 272) mentions that American software developer Philip Zimmermann released his encryption software *Pretty Good Privacy* (PGP) online to the public. The fact that there are programs available, such as PGP, to counter the effects of privacy infringements indicates that there is

a problem lurking in the domain of the current practices associated with cybersurveillance.

Conclusively, this paper has addressed surveillance from contrasting theoretical and hypothetical positions, illuminating its ability to cast both a positive and negative impact on individuals who are exposed to it. This has been shown through discussions that indicate the possible detrimental impact of data collection on individual privacy and liberty. Various authors have been included in these discussions in order to provide a well-informed and integrative explanation of how relational surveillance is not proportionate in many cases and therefore fails to achieve its full potential in contributing to improving issues of cybercrime.

References

- Alana Saulnier (2017) Surveillance as Communicating Relational Messages: Advancing Understandings of the Surveilled Subject. *Surveillance & Society* 15, (2) 286–302. Available at: https://doi. org/10. 24908/ss. v15i2. 6334 [Accessed 3 January 2019].
- Benoît Dupont (2008) Hacking the panopticon: Distributed online surveillance and resistance. In: *Sociology of Crime Law and Deviance* Vol. 10. Bingley: Emerald (MCB UP)https://doi. org/10. 1016/S1521-6136(07)00212-6[Accessed 6 January 2019].
- Connor Sheridan (2016) *Foucault, Power and the Modern Panopticon* , Senior Thesis. Trinity College, Hartford Connecticut. Available at: http://digitalrepository. trincoll. edu/theses/548.
- David Lyon (2001) *Surveillance Society: Monitoring Everyday Life* . 1st Edn. Buckingham [England]; Philadelphia: Open University Press.

- David Lyon (2007) *Surveillance studies: An Overview* . Cambridge, UK; Malden, MA: Polity.
- David Nelken (2014) Response 3: The logics of security: A comment on Valverde. *Criminology & Criminal Justice* 14, (4) 405–411. Available at: https://doi. org/10. 1177/1748895814541902[Accessed 3 January 2019].
- Economic Times (/2019) Cryptography – What is Cryptography? *The Economic Times* . Available at: https://economictimes. indiatimes. com/definition/cryptography.[Accessed 3 January 2019].
- Katherine J. Strandburg (2008) *Freedom of Association in a Networked World: First Amendment Regulation of Relational Surveillance* , SSRN Scholarly Paper No. ID 1136624. Rochester, NY: Social Science Research Network Available at: https://papers. ssrn. com/abstract= 1136624.[Accessed 7 January 2019].
- Kirstie Ball (2009) Exposure: Exploring the subject of surveillance. *Information, Communication & Society* 12, (5) 639–657. Available at: https://doi. org/10. 1080/13691180802270386[Accessed 7 January 2019].
- McCahill, M., and Finn, R. L. (2014) *Surveillance, Capital and Resistance: Theorizing the Surveillance Subject* . 1 edition. New York: Routledge.
- Michel Foucault (1975) *Discipline and Punish: The Birth of the Prison* . Trans. By Alan Sheridan 2nd, reprint Edn. Peregrine books.
- Randy Lippert (2008) David Lyon, Surveillance Studies: An Overview. *Canadian Journal of Sociology* 33, (1).

- Rick A. Matthews, and David Kauzlarich (2007) State crimes and state harms: a tale of two definitional frameworks. *Crime, Law and Social Change* 48, (1) 43–55. Available at: https://doi. org/10. 1007/s10611-007-9081-5[Accessed 10 January 2019].
- Robert H. Sloan, and Richard Warner (2016) *Relational Privacy: Surveillance, Common Knowledge, and Coordination* , SSRN Scholarly Paper No. ID 2864663. Rochester, NY: Social Science Research Network Available at: https://papers. ssrn. com/abstract= 2864663.[Accessed 11 December 2018].
- Simson L. Garfinkel, Jeffrey I. Schiller, Erik Nordlander, David Margrave, and Robert C. Miller (2005) Views, Reactions and Impact of Digitally-signed Mail in e-Commerce. In: *Proceedings of the 9th International Conference on Financial Cryptography and Data Security* . Berlin, Heidelberg: Springer-Verlaghttps://doi. org/10. 1007/11507840_18[Accessed 11 December 2018].
- Stephen J. Miller (1995) *Civilizing Cyberspace: Policy, Power, and the Information Superhighway* . Digital Print Ed edition. Addison Wesley.
- Thomas McMullan (2015/23/July) What Does the Panopticon Mean in the Age of Digital Surveillance? *The Guardian* (23). Available at: https://www. theguardian. com/technology/2015/jul/23/panopticon-digital-surveillance-jeremy-bentham.[Accessed 11 December 2018].