We Are Sleepwalking into a Surveillance Society': A Critical Analysis of Richard Thomas' Prediction in the Context of Contemporary Surveillance, Dataveillance, and Legal Safeguards

By

Ebele Kponam Newton
Department of History and Diplomacy,
Niger Delta University, Amassoma, Bayelsa State

&

Areprekumor Clinton
Department of History and Diplomacy,
Niger Delta University, Amassoma, Bayelsa State

Abstract

This study critically evaluates Richard Thomas's 2004 claim that the UK is "sleepwalking into a surveillance society," paying particular emphasis to modern methods of data monitoring, the laws governing them, and the associated privacy guarantees. With the recent high-profile privacy breaches and growing public anxiety about data management, the goal is to determine whether the widespread, sophisticated monitoring systems that have developed around the world are appropriate for Thomas's prognosis. The methodology involves a thorough evaluation of secondary sources, including scholarly journals, policy papers, and news items, which are subsequently analysed using Braun and Clarke's reflective thematic analysis. According to findings, governments' introduction of new legislative frameworks to enable them to engage in dataveillance at the expense of individuals' privacy has resulted in a significant increase in surveillance and dataveillance activities. Prominent examples of this include the US Patriot Act, the UK's Investigatory Powers Act, and extensive monitoring programs in nations like China and India. This research leads one to conclude that state control has gained an advantage in the security-privacy balance, largely fulfilling Thomas's prediction. The continuous infringement of individuals' privacy rights is caused by the normalisation of monitoring techniques and the absence of adequate legal safeguards.

Keywords: **Sleepwalking, Surveillance, Legal Safeguards, Security, Society.**

Introduction

When considered from the standpoint of monitoring, privacy and security are two related but seemingly opposed concepts. Surveillance systems have become widespread, largely due to the efforts of governments and corporations monitoring occurrences in order to discourage potential dangers. However, the collection and preservation of personal information raises significant concerns regarding individual privacy because it may lead to misuse and discrimination (Lyon, 2018). Because people may self-censor due to the fear of being watched, the terrifying power of surveillance may alter people's behaviour (Bennett & Raab, 2018). Furthermore, the public's trust can be damaged and abuses of power might arise from the lack of transparency and accountability in monitoring procedures (Zuboff, 2019). Thus, while surveillance might increase security, it also gravely jeopardises privacy, necessitating strict regulation and clearly stated guidelines to strike a balance between these conflicting goals (Solove, 2021).

The former UK Information Commissioner, Richard Thomas, issued a warning in 2004 that the country was "sleepwalking into a surveillance society" due to worries about the dangers connected to the widespread use of surveillance and possible threats to individual privacy rights. Twenty years after Thomas's caution, the topic of surveillance remains highly relevant and hot. Concerns about the privacy implications of surveillance have intensified even further, partly due to the rise in technology use and data collection methods used by governments and businesses. There are two primary elements contributing to this: the first is the legal disputes over unauthorized data access and use involving Internet companies such as Google and Facebook, among others; the second is the increasing worries about privacy as indicated by online surveys.

Taking consideration of the afore-stated issues and the broad based concerns about dataveillance, this study aims to investigate if Richard Thomas' 2004 prediction about entering a surveillance society has come to pass. To answer the question, the research looks at current data-gathering and surveillance capabilities, data-gathering legislation, and global privacy protection measures that are currently in place. It makes considerable use of secondary sources, such

as scholarly papers, news media reports, policy documents, and regulations. The researcher actively engages with the data to uncover patterns and themes in the analysis process, which is based on Braun and Clarke's reflexive thematic analysis.

Thomas' Warning

He issued this warning in response to the UK government's plans for enormous databases, including those that would track children from birth to age 18 and create a demographic registry and national identity cards. With the use of these technologies, vast amounts of personal data might be gathered and made available to several authorities without the individuals' knowledge, leading to serious privacy violations (The Guardian, 2004). Thomas emphasised that excessive monitoring might result in decisions that directly impact people's lives being made based on possibly inaccurate data, creating a "climate of suspicion" and undermining public faith in governmental institutions (London Evening Standard, 2006). In addition, he drew parallels with authoritarian regimes and issued a warning that unchecked surveillance will lead to a society where the state possesses extensive personal data on people, reminiscent of the Cold War practices in Eastern Europe (Statewatch, 2006).

Contemporary Surveillance and Dataveillance Powers

Dataveillance and surveillance are related concepts that reflect the developments of the digital era. Surveillance, traditionally associated with state efforts to maintain law and order, is the act of attentively studying individuals or groups (Lyon, 2018). Conversely, dataveillance, a term used by Clarke (1988), refers more precisely to the continuous gathering and observation of data, particularly on the internet, encompassing metadata generated by digital exchanges in addition to the content of communications (van Dijck, 2014). Contemporary concerns centre largely on dataveillance, which is considered a more intensified version of surveillance. This paper argues that a major factor contributing to the expansion of data surveillance is the legal authority granted to it by various nations worldwide.

The United States' post-9/11 security concerns led to a significant evolution in monitoring methods even before 2004. To combat terrorism and criminality, these worries led governments all over the world to implement more comprehensive

surveillance programs (Naylor, 2017). This was accompanied by the introduction of fitting legislations, as evident in countries across the world.

- In the US, there is the USA Patriot Act and the Foreign Intelligence Surveillance Act (FISA) introduced after 9/11 (Greenwald, 2014). These laws allowed for the monitoring of foreign intelligence targets. Also, the US National Security Agency (NSA), which was primarily established by these legal powers, has a reputation for extensive data surveillance methods, such as gathering phone metadata on a huge scale and keeping a log of internet users' activity (Grenwald 2014).

- In the UK, dataveillance and is mainly governed by the Investigatory Powers Act 2016 (sometimes known as the "Snooper's Charter"), which gives law enforcement and intelligence services the authority to intercept communications and gather personal information about individuals (Liberty 2016). There is also extensive use of closed-circuit television (CCTV) with integrated facial recognition technology in public areas (Fussey et al., 2020).

- In China, high-tech tools (facial recognition cameras, artificial intelligence, and big data analytics), are used to monitor people and record their activities. The Chinese Cybersecurity Law and the social credit system are closely linked to the Chinese government's data surveillance capabilities (Creemers 2018) Companies and enterprises operating in China are required by the 2017 Chinese Cybersecurity Law to retain customer data domestically and grant government access to that data upon request (Zeng 2019).

- In India, the Central Monitoring System (CMS) enables the Indian government to watch over and intercept ICT communications in real-time without a court warrant (CIPESA 2021). India has strengthened data surveillance even further via the Information Technology Act (2000), which gives the Indian government the power to prohibit websites and online content deemed offensive. There is also the Aadhaar system in India, which assigns residents unique identifying numbers based on biometric data.

- In Australia, the Telecommunications (Interception and Access) Act 1979 gives law enforcement the authority to access metadata and stored conversations without a warrant in some situations (Australian Government (2020). Technology companies are required by a later statute to help law enforcement access encrypted data (Cameron 2019).

- There are similar laws across Africa. For example, in South Africa, law enforcement agencies are permitted to intercept conversations and gather metadata under the Regulation of Interception of conversations and Provision of Communication-Related Information Act (RICA) (CIPESA 2021). Comparably, Nigeria's Cybercrime Act permits law enforcement to access and monitor electronic communications, while Kenya's Information and Communications Act grants the government the authority to monitor and intercept communications (CIPESA, 2021). Also, Uganda grants the state access to and monitoring of communications and user data through the Uganda Communications Act.

In addition to the power and methods of data surveillance at the state level, huge organisations have also become well-known for a number of data surveillance initiatives that heavily leverage technology. Notably, data collection, analysis, and use of personal information is done by internet giants such as Google, Facebook, and Amazon using a variety of data surveillance tactics. Utilising tracking technology, like cookies, to monitor users' online activity across several websites is one form of data monitoring that these websites engage in. The resulting comprehensive user profiles are produced by combining all of this data, allowing for the creation of targeted advertising campaigns (Zuboff, 2019). Providers can better monitor user behaviour in real time by obtaining permission from users for mobile applications to access personal data, such as contacts and location information. Consumers who sign long terms of service agreements—which are rarely carefully read—often unwittingly consent to these tactics (European Commission, 2020). Moreover, data brokers gather and market customer data from publicly accessible records and social media, among other sources, building an intricate web of data surveillance that is generally undetectable to customers (Cohen, 2020).

Data Protection Laws and their Limitations

With widespread concerns about data protection, as evident in Richard Thomas' position, states everywhere have introduced legislations to protect individuals' privacy. For instance, the European Union's General Data Protection Regulation (GDPR), which went into effect in 2018, places a strong emphasis on principles like limiting data collection, ensuring accountability, and giving people the ability to see, edit, or delete their personal data. Standards for businesses handling data on EU individuals are provided by this rule. The California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA), two state laws that provide residents control over their personal information, are also in effect. According to these legislation (Mureithi, 2024; Netwrix, 2023), citizens have the right to know what data is being gathered and the option to refuse having their data sold. In Brazil's, there is the General Data Protection Law (LGPD), which is applicable to Brazilian businesses handling personal data. China's Personal Information Protection Law (PIPL), introduced in November 2021, establishes a comprehensive framework for handling personal data. The Privacy Act of 1988 governs the collection and use of personal data by governmental and nongovernmental organisations in Australia. Numerous other African nations (such as South Africa, Kenya, Nigeria, and Uganda) have also passed laws pertaining to data protection. The Malabo Convention on Cybersecurity and Personal Data Protection mandates that African Union member states create and implement strong data protection laws (Mureithi, 2024; Netwrix, 2023). On a global level, the UN has also emphasised how crucial international cooperation is in preventing overzealous data surveillance. Numerous United Nations resolutions that were passed between 2013 and 2018 emphasise the need of protecting privacy online (United Nations, 2013; United Nations, 2014; UN, 2016; UN, 2018). These resolutions demand that states prioritise privacy and express concern about the impact that surveillance and dataveillance have on human rights. Despite these laws, dataveillance remains a major issue of concern globally.

Waking up in a Surveillance State

A couple of years subsequent to voicing apprehensions regarding sleepwalking into a surveillance state, the UK commissioner conveyed concerns over awakening in such a situation. This worry was a sign that, only two years after the alert, some believed the prophesy had already come to pass. He is reported as saying this:

> I worry that a monitoring society is actually what we are awakening to today. The collection, sharing, and usage of ever-increasing amounts of information invades our personal space and results in decisions that have a direct impact on people's lives. Erroneous information or conclusions, security breaches, false matches and other identity-related incidents, and suspicions regarded as fact can all be generated with ease and have grave repercussions (cited in Conservatives Party 2009).

If Thomas's assessment that his forecast had come true by 2004 was debatable, then many of the points of contention are eliminated by the evidence of modern data surveillance methods, authorities, and legislation. Following Thomas's remarks, the UK's surveillance landscape underwent a significant transformation with the enactment of the Investigatory Powers Act (IPA) in 2016, popularly referred to as the "Snooper's Charter." This legislation, which aims to enhance accountability in state surveillance (CSIS, 2024), formalised significant powers for law enforcement and intelligence agencies to intercept communications and obtain metadata.

Provisions under the Investigatory Powers (Amendment) Act 2024 have worried privacy campaigners since they expand government surveillance capabilities and jeopardise the protections that were first put in place (Privacy Matters, 2024). Critics argue that these innovations may lead to mass monitoring tactics that lack sufficient checks and balances on government authority.

Beyond the UK, worldwide expansion of surveillance and dataveillance points even more toward the reality Thomas Richard's pessimistic forecasts already reflect. Particularly after the National Security Law was passed in 2020, which codified great powers to monitor citizens, especially in Hong Kong, under the pretense of preserving public order, the government's surveillance powers have expanded greatly in China (Harvard International Review, 2020). Mass monitoring and data collecting made possible by this legislation let authorities monitor people and quell opposition. Emphasizing the rising normalizing of surveillance in daily life, companies and business organizations are pushing in the United States to increase the use of face recognition technology for police and border security (Harvard International Review, 2020). Given the absence of

thorough government rules controlling their deployment, the use of such technology begs questions about privacy and civil liberties. Provisions enabling the internal security agency to trace the transmission of the virus by monitoring and collecting mobile phone location data let the Israeli government respond to the COVID-19 epidemic. This practice shows how health emergencies could hasten the acceptance of monitoring practices that might last long after the crisis has gone (Harvard International Review, 2020).

Moreover, the emergence of cross-border monitoring is becoming more and more common as governments spy on people living abroad without clear legislative control for such activities. This tendency affects the interaction between governments and people as many nations lack limits on international monitoring, therefore allowing possible invasions of private rights (Harvard International Review, 2020).

With these diverse laws permitting the government to access private data, there are extensive concerns about privacy among citizens globally. For example, in a research conducted in 2024 by TrustArc, 73% of consumers say they are more concerned about data privacy now than they were a year ago, and 79% of them say they are anxious about how their personal information is utilised. 60% of Americans think it is difficult to go about daily life without being watched by businesses and the government, which reflects a general sense of monitoring (Pew Research Centre, 2024). To this growing dissatisfaction is added the belief that more than half (59%) of consumers know very little about how their data is handled (Pew Research Centre, 2024). These privacy concerns are accompanied by intensification of calls for oversight over personal data use (TrustArc 2024).

Contemporary concerns over dataveillance transcend governments' access and use of data to include the actions of big corporations, which has resulted in major scandals and litigations globally. The Facebook-Cambridge Analytica scandal is one of the most well-known examples, wherein political advertising utilised private information obtained without consent from around 87 million individuals (Zengler, 2020). Aside from the outrage of the public, this incident led to Facebook being fined $5 billion by the Federal Trade Commission for privacy violations (Kang, 2019). Further casting doubt on Facebook's ability to protect user data is

another incident the corporation was embroiled in in 2021: the theft of data from over 500 million users, which was subsequently leaked online (Graham, 2021). Another significant internet company that has raised concerns about privacy is Google. Google is being sued by forty states in the US for allegedly using deceptive location tracking techniques to violate user privacy. The complaint claimed that Google continued to collect private data even after users disabled location tracking, which led to a $392 million record (The Science Survey, 2023). Concerns over user consent and data processing practices were raised by this issue, which also brought attention to Google's ambiguous location monitoring policies. Under the General Data Protection Regulation (GDPR) of the European Union, Google has also faced criticism; in 2019, the company was fined €57 million for not obtaining the necessary user consent for ad personalisation (The Science Survey, 2023).

Conclusion

The data presented in this paper highlights the alarming fact that Richard Thomas's 2004 prediction of the UK "Sleepwalking into a surveillance society" is now a reality. Individual private rights have been greatly lost as surveillance and dataveillance activities—made possible by governmental frameworks and technical developments—have grown. High-profile events involving large internet companies and the great powers given to governments around show how progressively state control dominates the balance between security and privacy. Public mistrust has resulted from the adoption of monitoring techniques as well as from lack of openness and responsibility. Furthermore, the terrifying effect of widespread monitoring on civil liberties as shown in many studies emphasizes the strong necessity of strong legal defenses and legislative systems to protect personal freedoms. The results imply that the trend toward an ever more invasive monitoring society would persist without significant change and active engagement from stakeholders, hence further breaching the fundamental ideas of liberty and privacy. This makes it necessary for initiatives aiming at creating greater legal and institutional protections as well as increasing public debate stressing individual privacy and rights alongside security needs.

References

ACLU, 2021. The USA PATRIOT Act: A Summary. [online] Available at: https://www.aclu.org/other/usa-patriot-act-summary [Accessed 20 August 2024].

Andrejevic, M., 2012. Surveillance and Alienation in the Online Economy. Theoretical Criminology, 16(3), pp. 85-102.

Austlii, 2023. Dataveillance Regulation: A Research Framework. [online] Available at: https://www6.austlii.edu.au/au/journals/JlLawInfoSci/2017/6.pdf [Accessed 20 August 2024].

Australian Government, 2020. Telecommunications (Interception and Access) Act 1979. [online] Available at: https://www.legislation.gov.au/Details/C2020C00048 [Accessed 20 August 2024].

Ball, K., Haggerty, K. D., & Lyon, D. (2018). Routledge Handbook of Surveillance Studies. Routledge.

BBC News, 2006. Britain is 'surveillance society'. [online] Available at: http://news.bbc.co.uk/2/hi/uk_news/6108496.stm [Accessed 20 August 2024].

Bennett, C. J., & Raab, C. D. (2018). The Governance of Privacy: Policy Instruments in Global Perspective. Ashgate.

Cameron, D., 2019. The Encryption Debate: What You Need to Know About the Assistance and Access Act. The Conversation. [online] Available at: https://theconversation.com/the-encryptiondebate-what-you-need-to-know-about-the-assistance-and-access-act-110098 [Accessed 20 August 2024].

CIPESA, 2021. Privacy Imperilled: Analysis of Surveillance, Encryption and Data Localisation

Laws in Africa. [online] Available at: https://cipesa.org/wp-content/files/briefs/PrivacyImperilled-Analysis-of-Surveillance-Encryption-and-Data-Localisation-Laws-in-AfricaReport.pdf [Accessed 20 August 2024].

Clarke, R., 1988. Information Technology and Dataveillance. Communications of the ACM, 31(5), pp. 498-512.

Conservatives Party, 2009. Reversing the Rise of the Surveillance State. 11 Measures to Protect Personal Privacy and Hold Government to Account.

Creemers, R., 2018. China's Social Credit System: A Socio-Technical Perspective. China Information, 32(2), pp. 123-145.

CSIS, 2024. A New Investigatory Powers Act in the United Kingdom Enhances Government Surveillance Powers. [online] Available at: https://www.csis.org/analysis/new-investigatorypowers-act-united-kingdom-enhances-government-surveillance-powers [Accessed 20 August 2024].

Dencik, L., et al. (2017). Data Justice: A New Framework for Understanding Data and Society. Data & Society Research Institute.

Fussey, P., et al., 2020. The Ethics of Using Facial Recognition Technology in Public Spaces. Journal of Information Ethics, 29(1), pp. 20-37.

Gonzalez, A., 2020. Twitter sued by widow of victim of terrorist attack. The Verge. [online] Available at: https://www.theverge.com/2020/10/27/twitter-lawsuit-terrorist-attack [Accessed 20 August 2024].

GOV.UK, 2023. New national security laws come into force. [online] Available at: https://www.gov.uk/government/news/new-national-security-laws-come-into-force [Accessed 20 August 2024].

Graham, A., 2021. Facebook data leak: What you need to know. TechCrunch. [online] Available at: https://techcrunch.com/2021/04/03/facebook-data-leak-what-you-need-to-know/ [Accessed 20 August 2024].

Greenwald, G., 2014. No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State. New York: Metropolitan Books.

Kang, C., 2019. Facebook fined $5 billion by FTC for privacy violations. The New York Times.

[online] Available at: https://www.nytimes.com/2019/07/24/technology/facebook-ftc-fine.html [Accessed 20 August 2024].

Liberty, 2016. The Investigatory Powers Act 2016. [online] Available at: https://www.libertyhumanrights.org.uk/issue/investigatory-powers-act-2016/ [Accessed 20 August 2024].

London Evening Standard, 2006. Warning over surveillance society. [online] Available at: https://www.standard.co.uk/news/uk/warning-over-surveillance-society-7186675.html [Accessed 20 August 2024].

Lyon, D. (2018). The Culture of Surveillance: Watching as a Way of Life. New York: New York University Press.

Lyon, D., 2018. The Culture of Surveillance: Watching as a Way of Life. New York: New York University Press.

Mureithi, C., 2024. The State of Data Protection Legislation in Africa. [online] Available at: https://www.techpolicy.press/the-state-of-data-protection-legislation-in-africa/ [Accessed 20 August 2024].

Netwrix, 2023. International Data Privacy Laws: A Guide. [online] Available at: https://blog.netwrix.com/2023/09/18/international-data-privacy-laws/ [Accessed 20 August 2024].

Pew Research Center, 2024. Public attitudes toward data privacy. [online] Available at: https://www.pewresearch.org [Accessed 20 August 2024].

Privacy Matters, 2019. UK Changes to UK Surveillance and Communications Law: The

Investigatory Powers Act 2024. [online] Available at:

https://privacymatters.dlapiper.com/2024/07/uk-changes-to-uk-surveillance-and-communications-law-the-investigatory-powers-amendment-act-2024/ [Accessed 20 August 2024].

Privacy Matters, 2024. UK Changes to UK Surveillance and Communications Law: The Investigatory Powers (Amendment) Act 2024. [online] Available at:

https://privacymatters.dlapiper.com/2024/07/uk-changes-to-uk-surveillance-and-communications-law-the-investigatory-powers-amendment-act-2024/ [Accessed 20 August 2024>.

Privacy Trends, 2024. The evolving landscape of privacy and trust. [online] Available at: https://www.privacytrends.com [Accessed 20 August 2024].

Sinha, A., 2020. Aadhaar and the Right to Privacy in India: A Critical Analysis. Journal of Law and Policy Review, 12(1), pp. 45-62.

Solove, D. J. (2021). Understanding Privacy. Harvard University Press

Statewatch, 2006. Waking up to a surveillance society. [online] Available at:

https://www.statewatch.org/media/documents/news/2006/oct/waking-up-to-a-surveillancesociety.pdf [Accessed 20 August 2024].

Surveillance Studies Network, 2021. Implications of Increased Surveillance on Civil Liberties in

the UK. [online] Available at: https://www.surveillance-studies.net/wpcontent/uploads/2021/06/SSN-Report-2021.pdf [Accessed 20 August 2024].

The Guardian, 2004. UK 'sleepwalking into Stasi state'. [online] Available at: https://www.theguardian.com/uk/2004/aug/16/britishidentity.freedomofinformation [Accessed 20 August 2024].

The Guardian, 2004. UK 'sleepwalking into Stasi state'. [online] Available at: https://www.theguardian.com/uk/2004/aug/16/britishidentity.freedomofinformation [Accessed 20 August 2024].

The Science Survey, 2023. The Problems of Internet Privacy and Big Tech Companies. [online] Available at: https://thesciencesurvey.com/news/2023/02/28/the-problems-of-internet-privacyand-big-tech-companies/ [Accessed 20 August 2024].

TrustArc, 2024. 2024 consumer privacy survey results. [online] Available at: https://www.trustarc.com [Accessed 20 August 2024].

United Nations, 2013. The Right to Privacy in the Digital Age. A/RES/68/167. [online] Available at: https://undocs.org/en/A/RES/68/167 [Accessed 20 August 2024].

United Nations, 2014. The Right to Privacy in the Digital Age. A/RES/69/166. [online] Available at: https://undocs.org/en/A/RES/69/166 [Accessed 20 August 2024].

United Nations, 2016. The Right to Privacy in the Digital Age. A/RES/71/199. [online] Available at: https://undocs.org/en/A/RES/71/199 [Accessed 20 August 2024>.

United Nations, 2018. The Right to Privacy in the Digital Age. A/RES/73/179. [online] Available at: https://undocs.org/en/A/RES/73/179 [Accessed 20 August 2024].

van Dijck, J., 2014. Datafication, dataism and dataveillance: Big Data. Big Data & Society, 1(1), pp. 1-12.

Zeng, J., 2019. China's Cybersecurity Law: Implications for International Business. Harvard International Law Journal, 60(1), pp. 1-30.

Zengler, T., 2020. The Cambridge Analytica scandal: What happened and why it matters. Harvard Business Review. [online] Available at: https://hbr.org/2020/03/the-cambridge-analytica-scandalwhat-happened-and-why-it-matters [Accessed 20 August 2024].

Zuboff, S. (2020). The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. PublicAffairs.

Zuboff, S., 2019. The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power, edn. *PublicAffairs, New York*.