Workplace surveillance and protection of worker's privacy in Covid-19

By Qingqin Zhang

Workplace surveillance and protection of worker's privacy in Covid-19

Abstract

Covid-19 forces more people to work from home and spawned new forms of employee surveillance. Employers can be much easier to monitor employees' activities and behavior through collecting, controlling, and processing employees' data and personal information through new technologies. Such surveillance can give rise to privacy concerns and challenges for human rights protection if it is excessive or not underpinned by a reasoned and proportionate interest in the workplace. This article will explain the workplace surveillance in practice and emphasis the necessity of protecting of employee's privacy right. After that, the existing protection of worker's privacy right under European Convention on Human Rights (ECHR) and the General Data Protection Regulation (GDPR) will be discussed combining with the case law. In the final section, this essay will analyze the challenge for protecting employees' right to privacy in Covid-19 and point out that the more stringent proportionality test and limited application of the principle of informed consent will better protect employees' privacy from excessive monitoring by their employers.

Introduction

Surveillance has been a feature of the workplace throughout history. The processing of employees' personal data ordinarily takes place not only during the employment, but also before the employment relationship is entered into for the purposes of recruitment, as well as after its termination, in connection with the obligation of record-keeping. During the recruitment phase, the employer can analyze the available information to reveal the novel, unexpected patterns, and profiles, and decide whether recruit the employees depending on these predictive results. After recruitment, the analysis of the biometric data and electronic communication information on social media plays a vital role in the employers' decision making. Employers log keystrokes,

interested in capturing when their employees use private services like Gmail, Facebook, and Twitter, and what they publish there.[1] In addition, employees use the mobile health (mHealth)[2] device would generate numerous personal health data, such as blood pressure, heart disease, insomnia, diabetes conditions. This data will be shared with his/her employer unknowingly or unwillingly, affecting the employee's privacy and non-discrimination rights[3]. At the end of the employment relationship, the processing of personal information by the former employer may continue - keeping employment records for a certain period. Although some forms of surveillance may serve legitimate interests, many others harm essential worker interests[4].

In COVID-19, the need for protecting workers' privacy becomes more urgent. One of the lasting impacts of the COVID-19 pandemic upon the world of work is likely to be a move away from the traditional workplace. Prior to the pandemic, the inability to engage in immediate supervision and control of the workforce may have rendered businesses reluctant to permit homeworking. There are only 5% of the workforce worked mainly form home according to the national statistics from 2019[5]. Social distancing and the lockdown measures adopted during the current Covid-19 health crisis have set homeworking as the new standard for many employees around the world. In an ONS survey in early

---

[1] Ifeoma Ajunwa and Kate Crawford and Jason Schultz, 'Limitless Worker Surveillance' (2017) 105 Calif L Rev 735, 9

[2] The World Health Organization (WHO) defines mHealth as 'medical and public health practice supported by mobile devices, such as mobile phones, patient monitoring devices, personal digital assistants (PDAs) and other wireless devices.', WHO Global Observatory for eHealth, New Horizons for Health through Mobile Technologies (World Health Organization 2011), 6, <https://www.who.int/goe/publications/goe_mhealth_web.pdf>, accessed 18 July 2021

[3] Céline Brassart Olsen, "To track or not to track? Employees' data privacy in the age of corporate wellness, mobile health, and GDPR", International Data Privacy Law 10(3), 237

[4] Michael Ford, 'Surveillance and Privacy at Work' (1998), The Institute of Employment Rights, 1

[5] Coronavirus and homeworking in the UK labour market: 2019, <https://www.ons.gov.uk/employmentandlabourmarket/peopleinwork/employmentandemployeetypes/articles/coronavirusandhomeworkingintheuklabourmarket/2019>, accessed 18 July 2021

May, 44% of adults surveyed were working from home now[6]. The trend suggests the home office, long regarded as a calmer place to work, may evolve into just another office fraught with the same constraints as a corporate cubicle.

Whilst surveillance methods have existed and been deployed for several years, there has been a massive surge in interest in their use during lockdown. For example, companies are employing strategies such as “taking photos of workers’ computer screens at random, counting keystrokes and mouse clicks and snapping photos of the workers at their computers” to surveil them. Further, companies monitor employees by artificial intelligence (AI) and machine learning (ML) technologies. Examples include features that generate reports about employee productivity or that scan employee communications to detect and provide real-time alerts of potential data security or other company policy violations. Even AI or ML monitoring programs can carry out the automated processing of personal data to evaluate certain aspects about an individual, including automatically notify management about potentially malicious activity by an employee, or that calculate and assign a security risk score to an employee based on their network activity to analyze or predict work performance based on the data collected.

Privacy is a fundamental human right, essential to autonomy and the protection of human dignity, serving as the foundation upon which many other human rights are built. The right to privacy protects people from the invasion of privacy that results from the use and disclosure of personal information collected and stored in computerized databases, often from the Internet[7]. In

---

[6] Coronavirus and the social impacts on Great Britain: 3 July 2020, <https://www.ons.gov.uk/peoplepopulationandcommunity/healthandsocialcare/healthandwellbeing/bulletins/coronavirusandthesocialimpactsongreatbritain/3july2020>, assessed 18 July 2021

[7] Gail Lasprogata and Nancy J King, 'Regulation of Electronic Employee Monitoring: Identifying Fundamental Principles of Employee Privacy through a Comparative Study of

addition to having the general value of personal data protection, the protection of workers' privacy rights contributes to the realisation of workers' or job seekers' rights to equality, freedom of expression and rights at work. Another reason for protecting employees' privacy right is related to the characteristics of labour relationship. The workers' right to privacy corresponds to the employer's right to information based on the right to manage the labour, which is a reciprocal relationship. Most employee contracts allow management the freedom to do whatever they want with the data collected from office-issued equipment.

The rapid expansion of technical on employee monitoring amplifies the intrusive nature of monitoring activities to increase company efficiency and innovation[8]. New surveillance technologies reinforce the asymmetries inherent between the parties in the employment relationship and give the employer a new source of power over the employee, namely information. This will create an apparent conflict of interest between the employer's right to surveillance and the employee's privacy. Moreover, the information asymmetry between data subjects and data controllers is exacerbated in the employment context by the general inequality of bargaining power between the parties to the employment relationship. Thus, it may not be easy to prove whether workers freely give informed consent of data collection or processing. In addition, excessive monitoring can result in organizational deviance and misconduct and break the trust between employees and employers, even affecting the long run of enterprises.

The EU employees' privacy protection framework and practice

Data Privacy Legislation in the European Union, United States and Canada' (2004) Stan Tech L Rev 4, 8

[8] Ifeoma Ajunwa and Kate Crawford and Jason Schultz, 'Limitless Worker Surveillance' (2017) 105 Calif L Rev 735, 743

At the EU level, the right to privacy protection is explicitly recognized by Article 8 of the EU Charter of Fundamental Rights[9] and the Lisbon Treaty. The Lisbon Treaty Article 16[10] provides a legal basis for rules on data protection for all activities within the scope of EU law. The Article 8 European Convention on Human Rights (ECHR) is another crucial provision for protecting employees' privacy right. The literal meaning of Article 8 ECHR seems no relationship with the employment context. However, the rise of modern technology with its sophisticated devices for surveillance and information storage triggered the ECtHR's heightened sensitivity to intrusions upon informational privacy[11]. Meanwhile, how to define the scope of privacy under ECHR Article 8 is crucial for protecting worker' s privacy. Lord Woolf in *R v Broadcasting Standards Commission ex parte BBC*[12] said: 'an interference with privacy is not even like an elephant, of which it can be said it is at least easy to recognize if not define.'The ECtHR held that work-related issues are involved in the protected private life under ECHR Article 8 in *Niemietz v Germany*[13]. In *Niemietz*[14], the court extend the notion of privacy from the personal life's 'inner circle' to the right to establish and develop relationships with other human beings to some degree. This interpretation is crucial for work-from-home people, whose professional activities cannot be distinguished from private life. If the scope of 'private life' is defined in the 'inner circle', the work-from-home workers' privacy right cannot be protected under ECHR Article 8. The ECtHR in *Halford v UK*[15] confirmed the argument in *Niemietz* and considered the application of article 8 ECHR explicitly in the typical

---

[9] Normally, the right to privacy guaranteed in article 7 of EU Charter of Fundamental Rights should not been seen as same right as the right to data protection; however, the European Court of Justice (ECJ) does not always make clear distinctions between article 7 and 8 of the Charter. The ECJ has not decide any specific cases about privacy protection of employees based on article 7 and 8 of the Charter.

[10] The Lisbon Treaty Article 16 paragraph (1) provided that every natural person has a subjective right to data protection.

[11] A Ieven, 'Privacy Rights as Human Rights: No Limits?' , at 315

[12] *R v Broadcasting Standards Commission ex parte BBC* [2000] 3 WLR 1327 at 1332.

[13] *Niemietz v Germany* (1993) 16 E.H.R.R. 97, [27]-[29].

[14] Ibid 13

[15] *Halford v United Kingdom* (1997) 24 E.H.R.R. 523, [1]-[2].

workplace area. The existing courts' stand is that telephone calls made from business premises may be covered by the notions of "private life" and "correspondence" under ECHR Article 8 (1). Some people would argue that employees who enter an employer's premises to do paid work have left 'private' space and entered a 'public' arena, where they should expect to be observed by their supervisors[16]. It is unreasonable that employees expect an absolute freedom from any monitoring in the workplace. In this case, the plaintiff, Halford, had the "reasonable expectation of privacy" for calls because of no warning of monitoring in advance. Therefore, the ECtHR held that the employees' right to privacy and correspondence was unjustifiably interfered with since the employer monitor employees' telephone calls at work.

Moreover, the decision of *Copland v UK*[17] confirms that Article 8(1) applies not only to telephone calls made from the workplace but also to e-mail and Internet usage. The ECtHR held that the collection and storage of personal information relating to her telephone calls, as well as her e-mail and Internet usage, without her knowledge, amounted to an interference with Ms Copland's right to respect for her private life. Therefore, the restrictions of employee's privacy should correspond with the standard – accessibility and foreseeability, the justification test[18] and proportionality both in public employment situations and private employment contracts. In other words, the infringement of employee's privacy should be proportional to the employers 'interest – the duty of loyalty and discretion of the employees. For those work-from-home people, the proportionality test should apply more rigid criteria since home is completely different from the privacy of the traditional office. In other words, the employees would have higher expectation of privacy in home. In the recent

---

[16] A Westin, Privacy and Freedom, (London: Bodley Head, 1967), at 276

[17] *Copland v United Kingdom* (2007) 45 E.H.R.R. 37, [39]-[49].

[18] ECHR Article 8(2) lists the legitimate aim for the justification test, such as the interests of national security, public safety, or the economic well-being of the country.

judgment of *Bärbulescu v Romania*[19], the Court found that a private employer's monitoring of an employee's use of the Internet, including by accessing private messages sent via Yahoo Messenger, violated the employee's private life[20]. In *Bărbulescu*, the Court found that states are required not just to show that an adequate legislative framework was in place to protect privacy in the workplace but also to ensure that national courts had offered an appropriate balance between the interests of employer and employee[21]. The case confirms that the existence and degree of privacy that an individual can reasonably expect in a particular setting remains key to assessing whether Article 8 has been violated. That expectation always determines the rigour of the balancing exercise conducted by the authorities.

In view of rapid technological developments, the EU adopted new legislation in 2016 to adapt data protection rules to the digital age. The General Data Protection Regulation (GDPR) become applicable to protect employees' privacy, repealing the Data Protection Directive. The GDPR established a detailed and comprehensive data protection system in the EU. The GDPR applies to personal data an employer collects through employee monitoring. Under GDPR, employers must consider whether the processing of personal data is indeed necessary and, if so, that such personal data are collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes and are adequate, relevant, and limited to what is necessary for those purposes. Employers should also consider appropriate retention periods for personal data collected and processed. These key principle for the processing, storage of employee's personal data under GDPR become more vital in COVID-19 since the common

---

[19] *Bärbulescu v Romania* [2016] IRLR 235

[20] Ibid 19, [74]-[81]

[21] Ibid 19, [121]-[122]

applied criteria of proportionality under ECHR Article 8 is still vigorous before arising the leading case law.

The challenge of protection workers' privacy in the COVID-19

The paradigm shift toward remote working began before the COVID-19 pandemic broke out. The local and national directives have confined large portions of the population to their homes since then[22]. Although the complex EU human rights framework has been developed to provide the high level of legal protection of the rights to privacy and data protection, the sudden proliferation of working from home and the associated increase in interest in online surveillance tools present a new challenge for the right to privacy. Surveillance while working at home has almost turned the original conceptual question of workplace privacy on its head. Whereas the initial struggle was often to consider the continued presence of privacy in public spaces, the most private areas are now subject to systematic intrusion from outside and become quasi-public through screenshots and constant tracking[23]. Monitoring was originally intended to enhance the management of employees and to assess their productivity, and monitoring of work-from-home employees may go beyond the employer's original intentions. Compared to the traditional workplace, monitoring during work at home would significantly reduce the potential for an individual's home to act as a space shielded from public view, potentially capturing a wider range of activities that may accompany homeworking and may easily blur into an individual's home life, for example by tracking or capturing sensitive information about other members of their family, including their children[24]. There is an even deeper concern when it relates to a

---

[22] Data protection and working remotely, <https://gdpr.eu/working-remotely-data-security/>, accessed 28 July 2021

[23] P Collins, 'The Right to Privacy, Surveillance-by-Software and the"Home-Workplace"', UK Labour Law Blog, 3 September 2020, available at < https://uklabourlawblog.com>, accessed 18 July 2021

[24] E Frantziou, 'The right to privacy while working from home ('WFH'): why employee monitoring infringes Art 8 ECHR', UK Labour Law Blog, 5 October 2020, available at <https://uklabourlawblog.com>, accessed 18 July 2021

person's home, at a time when a global public health emergency is placing a significant part of the workforce at risk of redundancy. Feelings of anxiety and helplessness, as well as the potential difficulty of accessing workplace representation whilst isolated from co-workers, further weaken the position of the employees during work from home.

How to balance the privacy needs of employees and the primary interests of employers is the fundamental question of how worker's rights to privacy and management interests in an efficient workplace[25] since the notion of "reasonable expectation of privacy" affects the scope of the protection of the right in question and set the benchmark for assessing employees' privacy infringements cases. Traditionally, the Court tends to allow the strong privacy protections of the home insofar as the physical space in which the violation has occurred continues to serve as a principal or significant residence or 'domicile' (including of a professional nature) at the time when the potential interference occurs. Similarly, the Court could follow this stand to protect employee's privacy right in future work-from-home cases. However, the high expectation of privacy afforded within the home does not give rise to absolute protection from outside incursions since the efficiency of employers working from home will be significantly affected. In addition to the general principles of lawfulness, fairness, necessity, and transparency in protecting personal information under GDPR, proportionality and procedural guarantees against arbitrariness were essential.[26] The labour law left room for negotiation between the parties to the employment contract from a regulatory perspective. Thus, it was generally for the parties themselves to regulate a significant part of the content of their relations. As stated, the inherently imbalanced structure of the employment relationship challenges the possibility of consenting to employer-mandated

---

[25] Michel Ford, "Two Conceptions of worker privacy" (2002) 31 ILJ 135, at 146.

[26] Butterworths Human Rights Cases, Volume 44, (Butterworths Law, 2018)at 19.

monitoring; the application of the principle of informed consent should be strictly restricted. Therefore, the work-from-home model would drive the Court to adopt the proportionality test to scrutinise the balance between employees' reasonable expectations of privacy and employers' demand to improve productivity at a higher level. An employee's consent alone should not be taken as the legal ground for the employer's processing of their personal information.

Conclusion

In conclusion, the COVID-19 generalised the work-from-home style and improved the work surveillance. Although the ECHR and GDPR provide an essential protection legal framework, the pandemic challenges the existing legal framework to protect employee privacy since the most private space-home turns into the quasi-public space through employers' intense surveillance. Therefore, based on ECHR Article 8 and GDPR's basic data protection principle, the more stringent proportionality test and limited application of the informed consent principle would better protect employee's privacy against excessive monitoring by employers. Work monitoring within reasonable limits can create a positive interaction between employer and employee in the long run.

Bibliography

Books

Alan W, *Privacy and Freedom*, (1st, London: Bodley Head, 1967)

Butterworths Human Rights Cases, Volume 44, (Butterworths Law, 2018)

Michael F, 'Surveillance and Privacy at Work', (The Institute of Employment Rights, 1998)

Otto, Marta. *The Right to Privacy in Employment: A Comparative Analysis.* (1st, Hart Publishing, 2016)

Schömann, I., Lörcher, K., *The European Convention on Human Rights and the Employment Relation*, (Bloomsbury Publishing, 2014)
Witzleb N and others (eds), *Emerging Challenges in Privacy Law: Comparative Perspectives* (Cambridge University Press, 2014)

Cases

R v Broadcasting Standards Commission ex parte BBC
Niemietz v Germany (1993) 16 E.H.R.R. 97
Halford v United Kingdom (1997) 24 E.H.R.R. 523
Copland v United Kingdom (2007) 45 E.H.R.R. 37
Bärbulescu v Romania [2016] IRLR 235

Journals

Ifeoma Ajunwa and Kate Crawford and Jason Schultz, 'Limitless Worker Surveillance' (2017) 105 Calif L Rev 735
Gail Lasprogata and Nancy J King, 'Regulation of Electronic Employee Monitoring: Identifying Fundamental Principles of Employee Privacy through a Comparative Study of Data Privacy Legislation in the European Union, United States and Canada' (2004) 2004 Stan Tech L Rev 4
Pauline T Kim, 'Collective and Individual Approaches to Protecting Employee Privacy: The Experience with Workplace Drug Testing' (2006) 66 La L Rev 1009
Marta Otto, 'Workforce Analytics v Fundamental Rights Protection in the EU in the Age of Big Data' (2019) 40 Comp Lab L & Pol'y J 389
George M Dery II, 'Trading Privacy for Promotion? Fourth Amendment Implications of Employers Using Wearable Sensors to Assess Worker Performance' (2020) 16 Nw J L & SocPol'y 17

Céline Brassart Olsen, “To track or not to track? Employees’ data privacy in the age of corporate wellness, mobile health, and GDPR”, International Data Privacy Law 10(3)

Gail Lasprogata and Nancy J King, 'Regulation of Electronic Employee Monitoring: Identifying Fundamental Principles of Employee Privacy through a Comparative Study of Data Privacy Legislation in the European Union, United States and Canada' (2004) 2004 Stan Tech L Rev 4

Ifeoma Ajunwa and Kate Crawford and Jason Schultz, 'Limitless Worker Surveillance’ (2017) 105 Calif L Rev 735

Michel Ford, “Two Conceptions of worker privacy” (2002) 31 ILJ 135

Website and blogs

E Frantziou, ‘The right to privacy while working from home (‘WFH’): why employee monitoring infringes Art 8 ECHR’, UK Labour Law Blog, 5 October 2020, available at <https://uklabourlawblog.com>

P Collins, ‘The Right to Privacy, Surveillance-by-Software and the “Home-Workplace”’, UK Labour Law Blog, 3 September 2020, available at < https://uklabourlawblog.com>

Kara K. Trowell, Proceed with Caution When Remotely Monitoring Employees in the EU, <https://www.lexology.com/library/detail.aspx?g=547a4439-d862-4a8b-9ffc-8164637c32a3>

WHO Global Observatory for eHealth, New Horizons for Health through Mobile Technologies (World Health Organization 2011) 6, <https://www.who.int/goe/publications/goe_mhealth_web.pdf>

Coronavirus and the social impacts on Great Britain: 3 July 2020, <https://www.ons.gov.uk/peoplepopulationandcommunity/healthandsocialcare/healthandwellbeing/bulletins/coronavirusandthesocialimpactsongreatbritain/3july2020>

Coronavirus and homeworking in the UK labour market: 2019, <https://www.ons.gov.uk/employmentandlabourmarket/peopleinwork/employmentandemployeetypes/articles/coronavirusandhomeworkingintheuklabourmarket/2019>

Data protection and working remotely, <https://gdpr.eu/working-remotely-data-security/>,