Written Evidence by Dr Adam Molnar, Danielle Thompson, and Dr Birgit Schippers (HRW0049)

Dear Members of the Joint Committee on Human Rights:

1. The Waterloo Cybersecurity and Privacy Institute (CPI) is an internationally recognized interdisciplinary research institute making significant impacts in improving information security and human privacy. The Strathclyde Centre for Internet Law and Policy (SCILP), which is based in the Strathclyde Law School, focuses on the legal challenges generated by new technologies.

2. This submission was prepared by Dr Adam Molnar and Danielle E. Thompson (CPI) and by Dr Birgit Schippers (SCILP).

3. The submission is guided by interdisciplinary research into the privacy and security impacts of employee monitoring software, funded by Canada's Social Sciences and Humanities Research Council (SSHRC). We acknowledge additional research support from Dr Urs Hengartner and Adam Campbell (CPI) that contributed to the preparation of this submission.

4. This submission describes what employee monitoring applications (EMAs) are, the risks they pose to privacy and information security, the concerns raised under Article 8 of the European Convention on Human Rights (ECHR), and the relationship of EMAs to existing safeguards in the UK.

Part 1: The Rise of EMAs

- EMAs are a type of digital surveillance software that enables employers to remotely monitor the behaviour of their workers. These applications track an array of employee activities including, but not limited to, keystrokes, mouse clicks, websites visited, applications used (including email and social media), desktop screenshots, audio and video surveillance, facial recognition, and GPS tracking. Some apps operate covertly. Data collected from employees are routed through the vendors servers and are made available to companies via cloud access.

- While companies may view EMAs as a helpful management tool that allows them to limit costs, minimise risks to cybersecurity, and maintain worker performance, the global influx of EMAs into private settings (including in homes and on personal devices) blurs conventional work-home boundaries and raises serious questions about the practical adequacy of privacy rights in the contemporary digital workplace.

Part 2: Article 8 Considerations

- The European Court of Human Rights (ECtHR) has addressed the practice of employee monitoring under **Article 8** of the Convention. The right to privacy in the office or place of work was first grounded in *Niemitz v Germany*[1]. In *Bărbulescu v Romania*, however, the court ruled that states are obligated to establish legal frameworks that safeguard employees' privacy in the workplace. They include:

  i. Monitoring must be **necessary** to achieve a certain aim.
  ii. Data must be collected for specified, explicit and **legitimate purposes**.
  iii. The employer must provide employees with full **notification** about monitoring operations.
  iv. Personal data being monitored must be **proportionate** in relation to the specified purpose.
  v. The employer is required to take all possible **security** measures to ensure that the data collected are not accessible to third parties.
  vi. **Adequate safeguards** must be in place to protect employees' rights, such as limiting access to monitoring data, ensuring that data is not used for purposes other than the stated legitimate aim, and deleting data when it is no longer needed.

- Any use of EMAs must be accompanied with a **notification** policy. It is important to note, however, that the mere existence of a notification to employees that EMAs are being used does not effectively remove an employee's reasonable expectation of privacy, nor does it alone abrogate their Article 8 right to privacy in workplace activities. Transparency is a necessary but insufficient remedy for the range of additional harms associated with EMAs.

- The use of EMAs to monitor remote workers **are neither necessary nor proportionate**. Given the extensive degree of intrusion into the private lives of individuals, less intrusive means to achieve the same outcomes may be used. Persistent monitoring of workers in their private homes, on privately owned devices which are often shared, represents some of the most intrusive means of technological surveillance that exist. We encourage the JCHR to focus on the viability of alternative and less-intrusive means of workplace supervision.

- While **legitimate** reasons for the adoption of EMAs in the remote workplace may relate to ‘economic well-being’ such as ‘productivity monitoring’ or ‘cybersecurity’, it should

[1] See also *Copland v UK (2007*), *Antović and Mirković v. Montenegro (2017)*

not be assumed that EMAs necessarily promote economic well-being. We are not aware of any scholarly research that demonstrates the positive impact that EMAs have for economic well-being compared with alternative means of supervision. In fact, our research into the cybersecurity and privacy weaknesses associated with these applications show that they could jeopardise economic well-being (along with public safety and national security).

- **Safeguards** do exist in the UK when it comes to the regulation of employee monitoring of remote workers through EMAs. They are, however, outdated, and ambivalent to the current realities of our technological environment and remote work.

Part 3: Safeguards and EMAs in the UK

- Our research is currently in the early stages of producing a comprehensive and detailed legal analysis of the use of EMAs in the UK and European context which is funded by the British Academy. We would welcome an opportunity to update the committee on this work in the coming months. The following section therefore is not intended to provide a comprehensive legal analysis of the existing regulatory environment in the UK regarding EMAs. Instead, we highlight specific areas of UK law that raise concern and that we hope might help direct the focus of the JCHR.

- The UK Data Protection Act 2018 (UK DPA) (i.e., the UK's implementation of the European Union's General Data Protection Regulations or EU GDPR) requires employers to obtain employee consent before engaging in monitoring through EMAs. Valid consent, however, is not always practical or feasible. Power imbalances between employers and employees mean that employees may feel coerced into giving their consent. Further, employees may not be aware of the full extent of the surveillance or the potential cybersecurity, privacy, and human rights risks they may be subject to with the use of EMA software.

- A notification regime however should not undermine an employee's reasonable expectation of privacy, and right to privacy, during work. Nor should it lead to the perception that merely because notification is given, monitoring through EMAs is necessary, proportionate, or aligned with legitimate aims.

- Employers are required to establish a lawful basis to gather and manage employees' sensitive data through EMAs in compliance with the UK DPA 2018. Most UK businesses using EMAs would likely consider the purpose and context of EMA monitoring as being connected to their 'legitimate interests'. This implies that any processing is considered

necessary for the legitimate interests of that company (or a third-party) unless the risks outweigh employees' rights. Notably, however, the UK Information Commissioner's Office (ICO) states that companies should avoid using legitimate interests if the monitoring occurs "in ways workers do not understand and would not reasonably expect, or if it is likely some workers would object if [their employer] explained it to them".[2]

- EMA monitoring, particularly in the working-from-home environment, infringes upon an employee's reasonable expectation of privacy. While it might be the case that employees expect their employers to supervise their work activities, they would not reasonably expect the scope of and sensitivity of information that is available through EMA monitoring to be collected and processed in the ways that it is.

- In our view, the use of EMA monitoring would fail the three-part test designed to secure a lawful basis for such monitoring in the DPA 2018. The three-part test includes a purpose test (whether there is a legitimate interest behind the processing), a necessity test (whether the processing is necessary for that purpose), and a balancing test (whether the legitimate interest is overridden by the person's interests, rights, or freedoms).

- While employers may have a legitimate interest to conduct monitoring (productivity, supervision, cybersecurity), the use of EMAs are not necessary for these purposes. Given the degree of sensitive data that are collected through EMA monitoring (including political opinions, trade union membership, biometric data, sexual orientation, and health or disability information), of an employee *as well as individuals they may communicate with,* an employee's rights and freedoms are severely jeopardised and not adequately balanced. Although outside the scope of this submission, we acknowledge that the use of EMAs also raises important issues under Article 14 of the ECHR.

- Sections 57 and 66 of the UK DPA (2018) require that any information gathered through monitoring should be protected and kept secure (e.g., pseudonymisation and data encryption). Our technical analysis of several EMAs indicates alarming security and privacy risks to companies and the employees that use EMAs. The types of data at risk can include intellectual property, employee records, sensitive personal health information, biometric data, and private communications (notably, including 'special category' data under the UK DPA 2018).

[2] UK ICO, 2022, *Employment Practices: Monitoring at Work draft guidance*, p.12 (October 12) https://ico.org.uk/media/about-the-ico/consultations/4021868/draft-monitoring-at-work-20221011.pdf

- The use of EMAs may also introduce legal liability under UK GDPR for companies (as data controllers) that use them to monitor their employees insofar as they are liable for the activities of commercial EMA vendor practices (as data processors). We would welcome the opportunity to share our technical findings with the JCHR in private.

Part 4: Recommendations

Considering the above concerns, we propose the following three recommendations:

i. A moratorium on the use of EMAs in the UK.

ii. Necessary revisions to UK GDPR and other relevant legislation to capture the novel privacy and security risks that EMAs pose in the contemporary workplace setting.

iii. The creation of a UK Workers Bill of Rights that outlines specific limits on device-level surveillance and enshrines a justiciable and enforceable worker's constitutional right to privacy in the workplace, based on principles of best practice in international human rights law.

11/04/2023